AWS Documento técnico

SageMaker Mejores prácticas de administración de Studio

SageMaker Mejores prácticas de administración de Studio: AWS Documento técnico

Table of Contents

SageMaker Mejores prácticas de administración de Studio

Fecha de publicación: 25 de abril de 2023 (Revisiones del documento)

Resumen

Amazon SageMaker AI Studio proporciona una única interfaz visual basada en la web en la que puede realizar todos los pasos de desarrollo del aprendizaje automático (ML), lo que mejora la productividad del equipo de ciencia de datos. SageMaker AI Studio le brinda acceso, control y visibilidad completos de cada paso necesario para crear, entrenar y evaluar modelos.

En este documento técnico, analizamos las mejores prácticas en temas como el modelo operativo, la administración de dominios, la administración de identidades, la administración de permisos, la administración de redes, el registro, la supervisión y la personalización. Las mejores prácticas que se analizan aquí están pensadas para la implementación empresarial de SageMaker AI Studio, incluidas las implementaciones multiusuario. Este documento está dirigido a administradores de plataformas de aprendizaje automático, ingenieros de aprendizaje automático y arquitectos de aprendizaje automático.

¿Usa Well-Architected?

El marco de AWS Well-Architected le ayuda a entender las ventajas y desventajas de las decisiones que toma al crear sistemas en la nube. Los seis pilares del marco le permitirán aprender las prácticas recomendadas de arquitectura para diseñar y utilizar sistemas fiables, seguros, eficientes, rentables y sostenibles. Mediante AWS Well-Architected Tool, disponible sin costo alguno en la AWS Management Console, puede comparar las cargas de trabajo con estas prácticas recomendadas respondiendo a una serie de preguntas para cada pilar.

En Machine learning Lens, nos centramos en cómo diseñar e implementar cargas de trabajo de ML en la Nube de AWS. Esta lente se suma a las prácticas recomendadas descritas en el Marco de Well-Architected.

Introducción

Cuando administra SageMaker AI Studio como su plataforma de aprendizaje automático, necesita orientación sobre las mejores prácticas para tomar decisiones informadas que le ayuden a escalar

su plataforma de aprendizaje automático a medida que aumentan sus cargas de trabajo. Para aprovisionar, poner en funcionamiento y escalar tu plataforma de aprendizaje automático, ten en cuenta lo siguiente:

- Elija el modelo operativo adecuado y organice sus entornos de aprendizaje automático para cumplir sus objetivos empresariales.
- Elige cómo configurar la autenticación de dominio de SageMaker AI Studio para las identidades de los usuarios y ten en cuenta las limitaciones a nivel de dominio.
- Decide cómo federar la identidad y la autorización de tus usuarios con la plataforma ML para realizar controles de acceso y auditorías detallados.
- Considere la posibilidad de configurar permisos y barreras para las distintas funciones de sus empleados de aprendizaje automático.
- Planifique la topología de su red de nube privada virtual (VPC) teniendo en cuenta la sensibilidad de su carga de trabajo de aprendizaje automático, la cantidad de usuarios, los tipos de instancias, las aplicaciones y los trabajos lanzados.
- Clasifique y proteja sus datos en reposo y en tránsito mediante el cifrado.
- Considere cómo registrar y monitorear las diversas interfaces de programación de aplicaciones (APIs) y las actividades de los usuarios para garantizar el cumplimiento.
- Personalice la experiencia del portátil SageMaker AI Studio con sus propias imágenes y scripts de configuración del ciclo de vida.

Modelo operativo

Un modelo operativo es un marco que reúne a las personas, los procesos y las tecnologías para ayudar a una organización a ofrecer valor empresarial de manera escalable, coherente y eficiente. El modelo operativo de aprendizaje automático proporciona un proceso de desarrollo de productos estándar para los equipos de toda la organización. Existen tres modelos para implementar el modelo operativo, según el tamaño, la complejidad y los factores que impulsan el negocio:

- Equipo de ciencia de datos centralizado: en este modelo, todas las actividades de ciencia de datos se centralizan en un solo equipo u organización. Esto es similar al modelo del Centro de Excelencia (COE), en el que todas las unidades de negocio recurren a este equipo para realizar proyectos de ciencia de datos.
- Equipos de ciencia de datos descentralizados: en este modelo, las actividades de ciencia de datos se distribuyen en diferentes funciones o divisiones empresariales, o en función de diferentes líneas de productos.
- Equipos de ciencia de datos federados: en este modelo, las funciones de servicios compartidos, como los repositorios de código, los procesos de integración y entrega continuas (CI/CD), etc., son gestionadas por un equipo centralizado, y cada unidad de negocio o función a nivel de producto está gestionada por equipos descentralizados. Esto es similar al modelo integrado, en el que cada unidad de negocio tiene sus propios equipos de ciencia de datos; sin embargo, estos equipos de unidades de negocio coordinan sus actividades con el equipo centralizado.

Antes de decidir lanzar su primer dominio de estudio para casos de uso de producción, considere su modelo operativo y las AWS mejores prácticas para organizar su entorno. Para obtener más información, consulte Cómo organizar su AWS entorno mediante varias cuentas.

La siguiente sección proporciona orientación sobre cómo organizar la estructura de la cuenta para cada uno de los modelos operativos.

Estructura contable recomendada

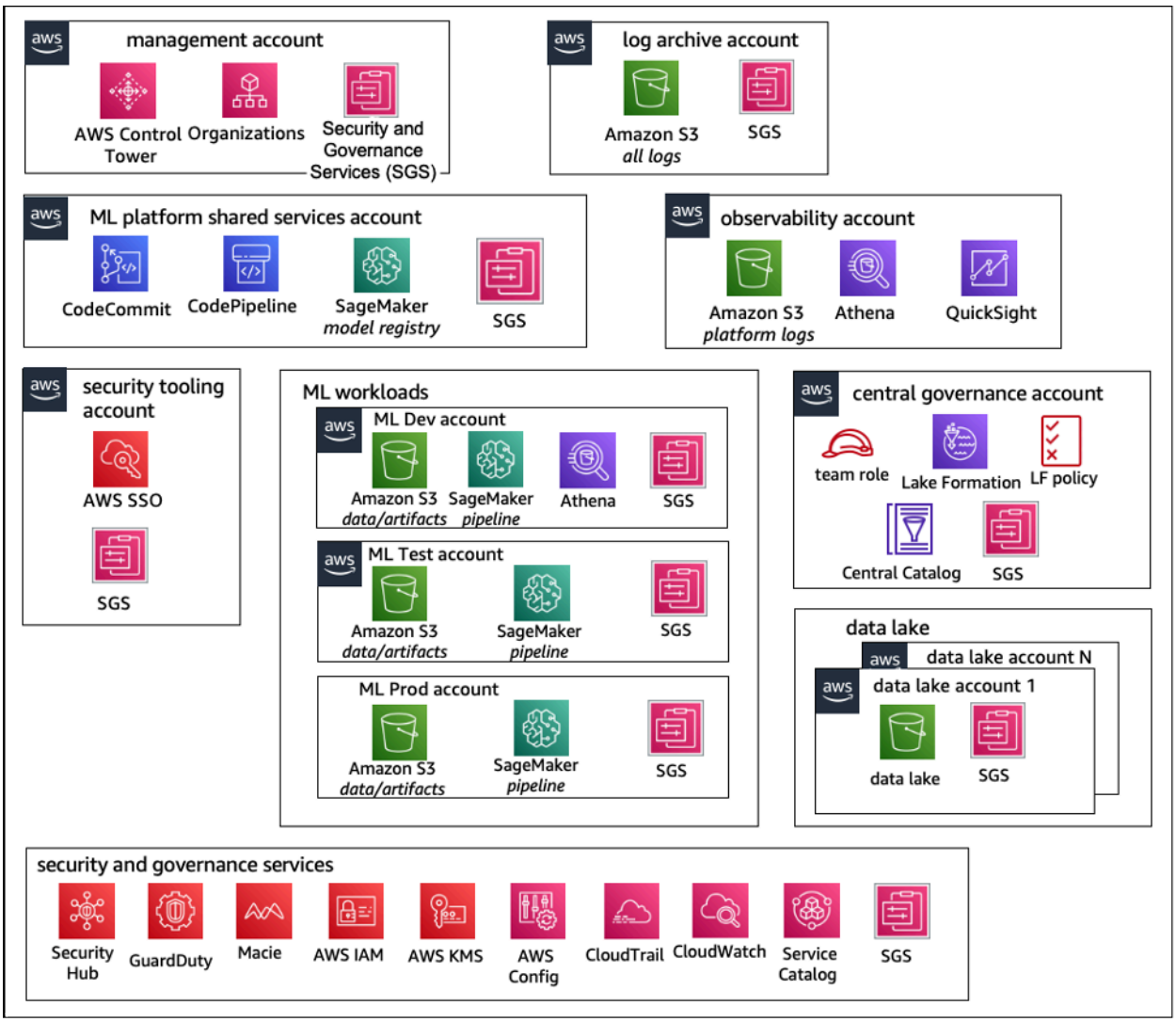
En esta sección, presentamos brevemente la estructura contable de un modelo operativo con la que puede empezar y modificar de acuerdo con los requisitos operativos de su organización. Independientemente del modelo operativo que elija, le recomendamos implementar las siguientes prácticas recomendadas comunes:

- AWS Control TowerÚselo para configurar, administrar y gobernar sus cuentas.
- Centralice sus identidades con su proveedor de identidad (IdP) AWS IAMe Identity Center con una cuenta de Securitiy Tooling de administrador delegado y permita el acceso seguro a las cargas de trabajo.
- Ejecute cargas de trabajo de aprendizaje automático con aislamiento a nivel de cuenta en todas las cargas de trabajo de desarrollo, prueba y producción.
- Transmita los registros de las cargas de trabajo de aprendizaje automático a una cuenta de archivo de registros y, a continuación, filtre y aplique el análisis de registros en una cuenta de observabilidad.
- Gestione una cuenta de gobierno centralizada para aprovisionar, controlar y auditar el acceso a los datos.
- Incorpore servicios de seguridad y gobierno (SGS) con las barreras preventivas y de detección adecuadas en cada cuenta para garantizar la seguridad y el cumplimiento, según los requisitos de su organización y de carga de trabajo.

Estructura de cuentas modelo centralizada

En este modelo, el equipo de la plataforma ML es responsable de proporcionar:

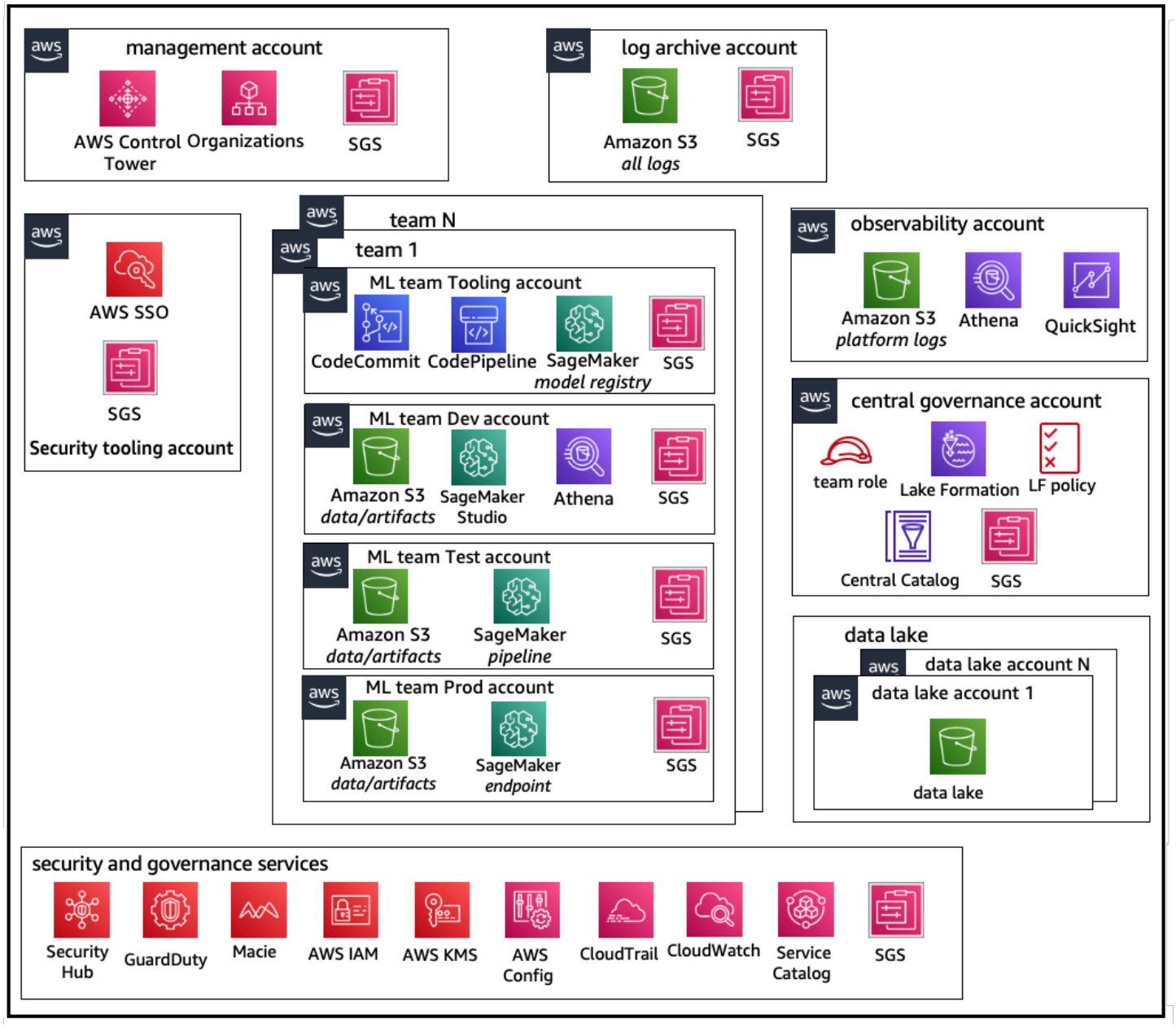
- Una cuenta de herramientas de servicios compartidos que aborda los requisitos de Machine Learning Operations (MLOps) de los equipos de ciencia de datos.
- Cuentas de desarrollo, pruebas y producción de cargas de trabajo de aprendizaje automático que se comparten entre los equipos de ciencia de datos.
- Políticas de gobierno para garantizar que la carga de trabajo de cada equipo de ciencia de datos se ejecute de forma aislada.
- Mejores prácticas comunes.



Estructura contable de un modelo operativo centralizado

Estructura contable modelo descentralizada

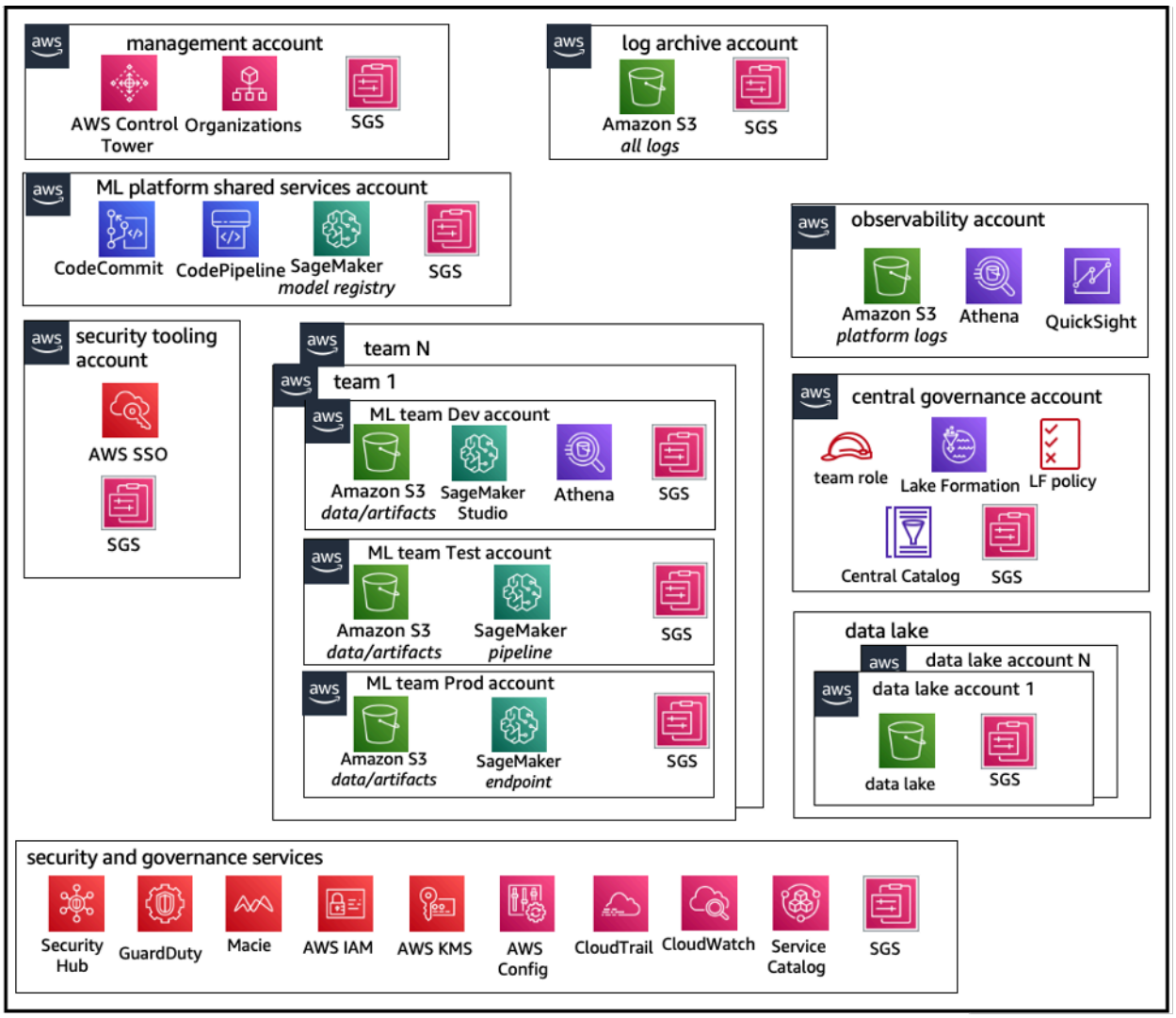
En este modelo, cada equipo de aprendizaje automático opera de forma independiente para aprovisionar, administrar y controlar las cuentas y los recursos de aprendizaje automático. Sin embargo, recomendamos que los equipos de aprendizaje automático utilicen un enfoque centralizado de observabilidad y gobernanza de datos para simplificar la gobernanza de los datos y la gestión de las auditorías.



Estructura contable de un modelo operativo descentralizado

Estructura de cuentas modelo federada

Este modelo es similar al modelo centralizado; sin embargo, la diferencia clave es que las cuentas de cada science/ML team gets their own set of development/test/production carga de trabajo de datos permiten un aislamiento físico sólido de sus recursos de aprendizaje automático y, además, permiten a cada equipo escalar de forma independiente sin afectar a los demás equipos.



Estructura contable del modelo operativo federado

Plataforma ML: multitenencia

La multitenencia es una arquitectura de software en la que una sola instancia de software puede atender a varios grupos de usuarios distintos. Un inquilino es un grupo de usuarios que comparten un acceso común con privilegios específicos a la instancia de software. Por ejemplo, si está creando varios productos de aprendizaje automático, cada equipo de producto con requisitos de acceso similares puede considerarse inquilino o equipo.

Si bien es posible implementar varios equipos en una instancia de SageMaker AI Studio (como SageMaker AI Domain), sopese esas ventajas y desventajas, como el radio de alcance, la atribución de costes y los límites de nivel de cuenta, al reunir varios equipos en un único SageMaker dominio

de AI Studio. Obtén más información sobre estas ventajas y prácticas recomendadas en las siguientes secciones.

Si necesitas un aislamiento absoluto de los recursos, considera la posibilidad de implementar dominios de SageMaker AI Studio para cada inquilino en una cuenta diferente. En función de tus requisitos de aislamiento, puedes implementar varias líneas de negocio (LOBs) como varios dominios dentro de una sola cuenta y región. Utilice los espacios compartidos para una colaboración prácticamente en tiempo real entre los miembros del mismo equipo/LOB. Con varios dominios, seguirás utilizando las políticas y los permisos de administración de acceso a la identidad (IAM) para garantizar el aislamiento de los recursos.

SageMaker Los recursos de IA creados a partir de un dominio se etiquetan automáticamente con el nombre de Amazon Resource Name (ARN) del dominio y el perfil o espacio del usuario ARN para facilitar el aislamiento de los recursos. Para ver ejemplos de políticas, consulte la documentación sobre el aislamiento de recursos de dominio. Allí podrá consultar la referencia detallada sobre cuándo utilizar una estrategia con varias cuentas o varios dominios, junto con las comparaciones de características de la documentación. También podrá ver ejemplos de scripts para rellenar las etiquetas de los dominios existentes en el repositorio. GitHub

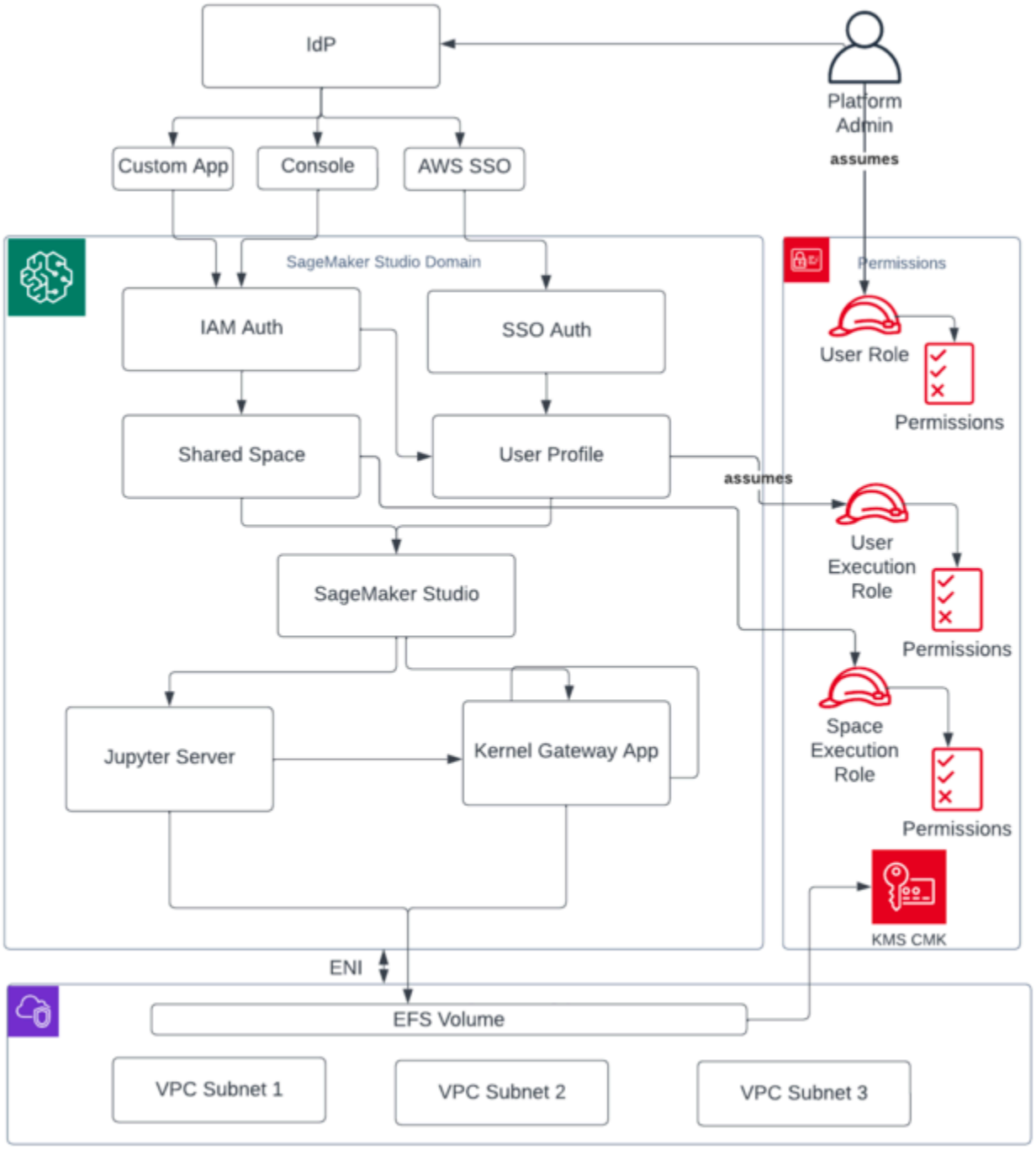
Por último, puede implementar un despliegue de autoservicio de los recursos de SageMaker AI Studio en varias cuentas utilizando. AWS Service Catalog Para obtener más información, consulta Administrar AWS Service Catalog productos en varios Cuentas de AWS y Regiones de AWS.

Administración de dominios

Un dominio Amazon SageMaker AI se compone de:

- Un volumen asociado de Amazon Elastic File System (AmazonEFS)
- Una lista de usuarios autorizados.
- Variedad de configuraciones de seguridad, aplicaciones, políticas y Amazon Virtual Private Cloud (AmazonVPC)

El siguiente diagrama proporciona una vista de alto nivel de los diversos componentes que constituyen un SageMaker AIStudio dominio:

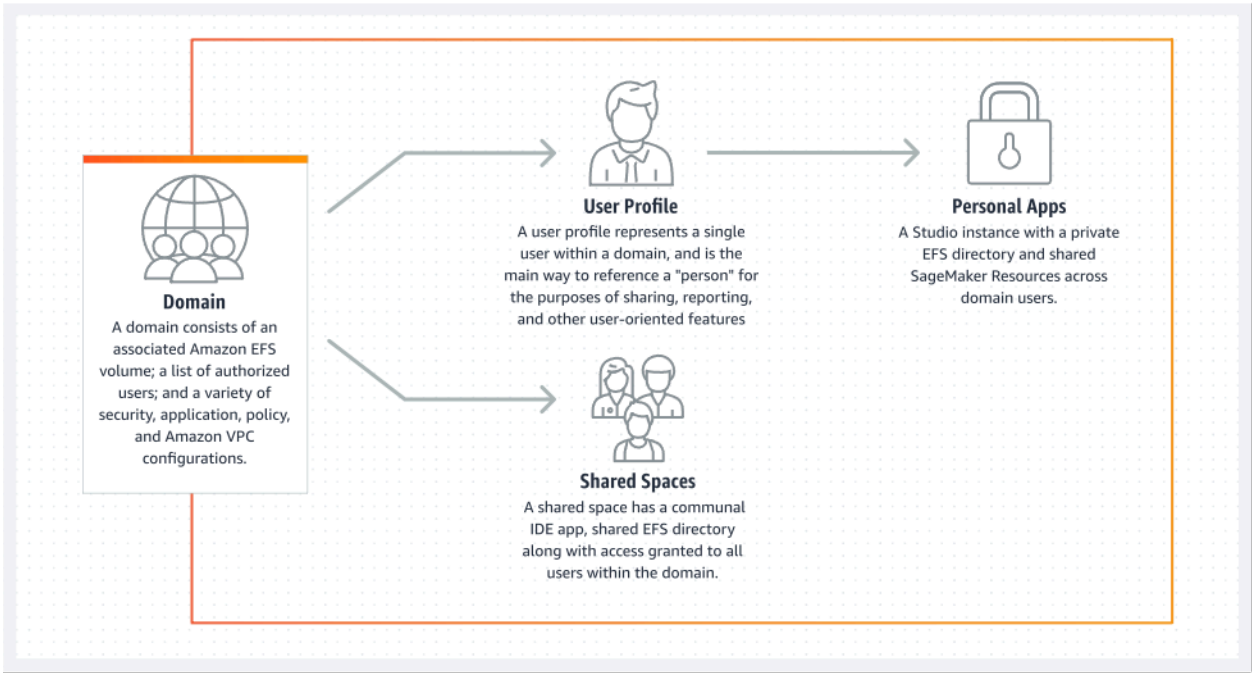


Vista de alto nivel de varios componentes que constituyen un dominio de SageMaker AI Studio

Varios dominios y espacios compartidos

Amazon SageMaker AI ahora admite la creación de varios dominios de SageMaker IA en uno solo Región de AWS para cada cuenta. Cada dominio puede tener su propia configuración de dominio, como el modo de autenticación, y una configuración de red, como VPC las subredes. Un perfil de usuario no se puede compartir entre varios dominios. Si un usuario humano forma parte de varios equipos separados por dominios, cree un perfil de usuario para el usuario en cada dominio. Consulte la Información general sobre varios dominios para obtener información sobre la reposición de etiquetas de los dominios existentes.

Cada dominio configurado en modo de IAM autenticación puede utilizar un espacio compartido para una colaboración entre usuarios prácticamente en tiempo real. Con un espacio compartido, los usuarios tienen acceso a un EFS directorio compartido de Amazon y a una JupyterServeraplicación compartida para la interfaz de usuario, y pueden coeditar prácticamente en tiempo real. El etiquetado automático de los recursos creados por los espacios compartidos permite a los administradores realizar un seguimiento de los costos a nivel de proyecto. La JupyterServer interfaz de usuario compartida también filtra recursos como los experimentos y las entradas de registro de modelos para que solo se muestren los elementos relevantes para la tarea de aprendizaje automático compartida. En el diagrama siguiente, se proporciona información general sobre las aplicaciones privadas y los espacios compartidos de cada dominio.



Información general sobre las aplicaciones privadas y los espacios compartidos dentro de un único dominio

Configura espacios compartidos en tu dominio

Por lo general, los espacios compartidos se crean para un proyecto o proyecto de aprendizaje automático en particular, en el que los miembros de un solo dominio requieren acceso casi en tiempo real al mismo almacenamiento de archivos subyacente yIDE. El usuario puede acceder a sus libretas de notas, leerlas, editarlas y compartirlas prácticamente en tiempo real, lo que le proporciona la forma más rápida de empezar a iterar con sus compañeros.

Para crear un espacio compartido, primero debe designar una función de ejecución predeterminada en el espacio que regirá los permisos de cualquier usuario que utilice el espacio. En el momento de escribir este artículo, todos los usuarios de un dominio tendrán acceso a todos los espacios compartidos de su dominio. Consulta Crear un espacio compartido para obtener la documentación más reciente sobre cómo añadir espacios compartidos a un dominio existente.

Configura tu dominio para la IAM federación

Antes de configurar la federación AWS Identity and Access Management (IAM) para tu dominio de SageMaker AI Studio, debes configurar un rol de usuario de IAM federación (como un administrador de plataforma) en tu IDP, tal y como se explica en la sección Gestión de identidades.

Para obtener instrucciones detalladas sobre cómo configurar SageMaker AI Studio con IAM esta opción, consulta Cómo integrar Amazon SageMaker Domain Using IAM Identity Center.

Configura tu dominio para la federación de inicio de sesión único () SSO

Para usar la federación de inicio de sesión único (SSO), debes habilitarla AWS IAM Identity Center en tu cuenta de AWS Organizationsadministración en la misma región en la que necesitas ejecutar AI Studio. SageMaker Los pasos de configuración del dominio son similares a los de IAM la federación, excepto que seleccionas AWS IAM Identity Center(iDC) en la sección de autenticación.

Para obtener instrucciones detalladas, consulta Cómo incorporar un SageMaker dominio de Amazon mediante IAM Identity Center.

SageMaker Perfil de usuario de AI Studio

Un perfil de usuario representa a un único usuario dentro de un dominio y es la forma principal de hacer referencia a una "persona" con el propósito de compartir, generar informes y otras características orientadas al usuario. Esta entidad se crea cuando un usuario incorpora toSageMaker AI Studio. Si un administrador invita a una persona por correo electrónico o la importa desde IdC, se crea automáticamente un perfil de usuario. Un perfil de usuario es el titular principal de la configuración de un usuario individual y tiene una referencia al directorio principal privado de Amazon Elastic File System (AmazonEFS) del usuario. Recomendamos crear un perfil de usuario para cada usuario físico de la aplicación SageMaker AI Studio. Cada usuario tiene su propio directorio dedicado en Amazon EFS y los perfiles de usuario no se pueden compartir entre dominios de la misma cuenta.

Cada perfil de usuario que comparte el dominio de SageMaker AI Studio recibe recursos de cómputo dedicados (como instancias de SageMaker IA de Amazon Elastic Compute Cloud (AmazonEC2)) para ejecutar cuadernos. Las instancias informáticas asignadas al usuario uno están completamente aisladas de las asignadas al usuario dos. Del mismo modo, los recursos informáticos asignados a los usuarios de una AWS cuenta son completamente independientes de los asignados a los usuarios de otra cuenta. Cada usuario puede ejecutar hasta cuatro aplicaciones (aplicaciones) en contenedores Docker aislados o imágenes en el mismo tipo de instancia.

Aplicación Jupyter Server

Cuando lanzas un bloc de notas de Amazon SageMaker AI Studio para un usuario accediendo al prefirmado URL o iniciando sesión con AWS IAM iDC, la aplicación Jupyter Server se lanza en la instancia gestionada por el SageMaker servicio de IA. VPC Cada usuario obtiene su propia aplicación dedicada de Jupyter Server en una aplicación privada. De forma predeterminada, la aplicación Jupyter Server para ordenadores portátiles SageMaker AI Studio se ejecuta en una *ml.t3.medium* instancia dedicada (reservada como tipo de instancia del sistema). El procesamiento de esta instancia no se factura al cliente.

La aplicación Jupyter Kernel Gateway

La aplicación Kernel Gateway se puede crear a través de la interfaz API o de SageMaker AI Studio y se ejecuta en el tipo de instancia elegido. Esta aplicación se puede ejecutar con una de las imágenes

integradas de SageMaker AI Studio que vienen preconfiguradas con los populares paquetes de ciencia de datos y aprendizaje profundo TensorFlow, como Apache MXNet y PyTorch.

Los usuarios pueden iniciar y ejecutar varios núcleos de portátiles Jupyter, sesiones de terminal y consolas interactivas en el mismo estudio. SageMaker image/Kernel Gateway app. Users can also run up to four Kernel Gateway apps or images on the same physical instance—each isolated by its container/image

Para crear aplicaciones adicionales, debes usar un tipo de instancia diferente. Un perfil de usuario solo puede tener una instancia en ejecución, de cualquier tipo de instancia. Por ejemplo, un usuario puede ejecutar tanto un bloc de notas simple con la imagen de ciencia de datos integrada de SageMaker AI Studio como otro portátil con la TensorFlow imagen integrada, en la misma instancia. A los usuarios se les factura por el tiempo que la instancia esté en ejecución. Para evitar costes cuando el usuario no ejecuta SageMaker AI Studio de forma activa, el usuario debe cerrar la instancia. Para obtener más información, consulta Cómo cerrar y actualizar las aplicaciones de Studio.

Cada vez que cierras y vuelves a abrir una aplicación de Kernel Gateway desde la interfaz de SageMaker AI Studio, esa aplicación se inicia en una nueva instancia. Esto significa que la instalación del paquete no se prolonga hasta que se reinicie la misma aplicación. Del mismo modo, si un usuario cambia el tipo de instancia en un portátil, se pierden los paquetes instalados y las variables de sesión. Sin embargo, puedes usar funciones como crear tu propia imagen y scripts de ciclo de vida para incorporar los paquetes del usuario a SageMaker AI Studio y conservarlos durante los cambios de instancia y el lanzamiento de nuevas instancias.

Volumen de Amazon Elastic File System

Cuando se crea un dominio, se crea un único volumen de Amazon Elastic File System (AmazonEFS) para que lo utilicen todos los usuarios del dominio. Cada perfil de usuario recibe un directorio principal privado dentro del EFS volumen de Amazon para almacenar las libretas, los GitHub repositorios y los archivos de datos del usuario. Cada espacio de un dominio recibe un directorio privado dentro del EFS volumen de Amazon al que pueden acceder varios perfiles de usuario. El acceso a las carpetas está segregado por usuario, mediante permisos del sistema de archivos. SageMaker AI Studio crea un identificador de usuario global único para cada perfil o espacio de usuario y lo aplica como una interfaz de sistema operativo portátil (POSIX) para acceder user/group ID for the user's home directory on EFS, which prevents other users/spaces a sus datos.

Copia de seguridad y recuperación

Un EFS volumen existente no se puede adjuntar a un nuevo dominio de SageMaker IA. En un entorno de producción, asegúrese de que se haya realizado una copia de seguridad del EFS volumen de Amazon (en otro EFS volumen o en Amazon Simple Storage Service (Amazon S3)). Si un EFS volumen se elimina accidentalmente, el administrador tiene que desmontar el dominio de SageMaker AI Studio y volver a crearlo. El proceso es el siguiente:

Realiza una copia de seguridad de la lista de perfiles de usuario, espacios y el EFS usuario asociado IDs (UIDs) a través de las `DescribeSpace` API llamadas `ListUserProfiles` `DescribeUserProfileList Spaces`, y.

1. Crea un nuevo dominio de SageMaker AI Studio.
2. Crea los perfiles y espacios de usuario.
3. Para cada perfil de usuario, copia los archivos de la copia de seguridad en EFS /Amazon S3.
4. Si lo desea, elimine todas las aplicaciones y los perfiles de usuario del antiguo dominio de SageMaker AI Studio.

Para obtener instrucciones detalladas, consulta la sección del apéndice Copia de seguridad y recuperación de dominios de SageMaker AI Studio.

> **Note**
>
> Esto también se puede lograr haciendo una `LifecycleConfigurations` copia de seguridad de los datos desde y hacia S3 cada vez que un usuario inicia su aplicación.

EBSVolumen de Amazon

También se adjunta un volumen de almacenamiento de Amazon Elastic Block Store (AmazonEBS) a cada instancia de SageMaker AI Studio Notebook. Se utiliza como volumen raíz del contenedor o la imagen que se ejecuta en la instancia. Si bien el EFS almacenamiento de Amazon es persistente, el EBS volumen de Amazon adjunto al contenedor es temporal. Los datos almacenados localmente en el EBS volumen de Amazon no se conservarán si el cliente elimina la aplicación.

Asegurar el acceso a los datos prefirmados URL

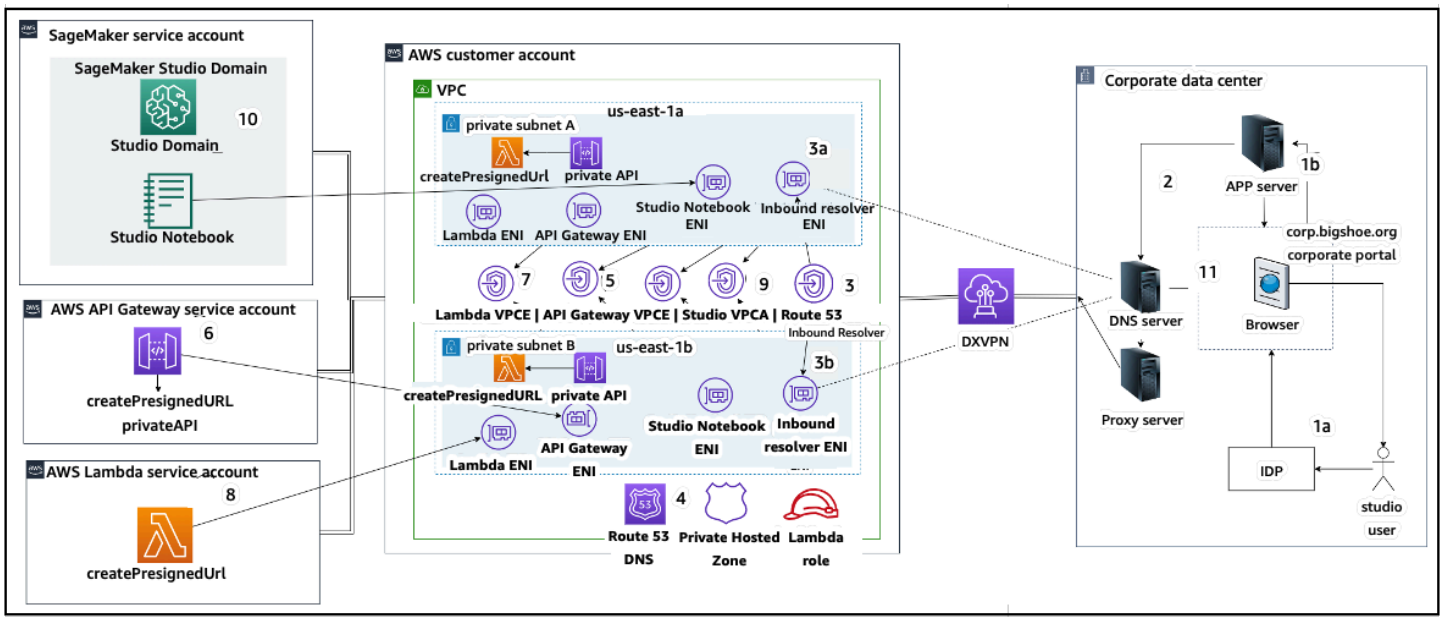
Cuando un usuario de SageMaker AI Studio abre el enlace del bloc de notas, SageMaker AI Studio valida la IAM política del usuario federado para autorizar el acceso y genera y resuelve la prefirmada URL para el usuario. Como la consola de SageMaker IA se ejecuta en un dominio de Internet, el dominio generado y prefirmado URL se puede ver en la sesión del navegador. Esto representa un vector de amenaza no deseado para el robo de datos y el acceso a los datos de los clientes cuando no se aplican los controles de acceso adecuados.

Studio admite algunos métodos para reforzar los controles de acceso contra el robo de datos prefirmadosURL:

- Validación de la IP del cliente mediante la condición de política IAM `aws:sourceIp`
- VPCValidación del cliente mediante la IAM condición `aws:sourceVpc`
- Validación del VPC punto final del cliente mediante la condición IAM de política `aws:sourceVpce`

Al acceder a los cuadernos de SageMaker AI Studio desde la consola de SageMaker AI, la única opción disponible es utilizar la validación de la IP del cliente con la condición `aws:sourceIp` de la IAM política. Sin embargo, puedes usar productos de enrutamiento de tráfico a través del navegador, como Zscaler, para garantizar la escalabilidad y el cumplimiento del acceso a Internet de tus empleados. Estos productos de enrutamiento de tráfico generan su propia IP de origen, cuyo rango de IP no está controlado por el cliente empresarial. Esto hace que sea imposible para estos clientes empresariales utilizar la `aws:sourceIp` condición.

Para utilizar la validación del VPC punto final del cliente mediante la condición de la IAM política`aws:sourceVpce`, la creación de un dispositivo prefirmado URL debe originarse en el mismo cliente en el VPC que se implementa SageMaker AI Studio, y la resolución del punto final prefirmado URL debe realizarse a través de un VPC terminal de SageMaker AI Studio instalado en el cliente. VPC Esta resolución de lo prefirmado URL durante el tiempo de acceso para los usuarios de la red corporativa se puede lograr mediante reglas de DNS reenvío (tanto en Zscaler como en la empresaDNS) y, luego, al punto final del cliente VPC mediante un solucionador de entradas Amazon Route 53, como se muestra en la siguiente arquitectura:



Acceso a Studio prefirmado URL con un VPC terminal a través de la red corporativa

Para obtener step-by-step instrucciones sobre la configuración de la arquitectura anterior, consulte Secure Amazon SageMaker AI Studio presigned URLs Part 1: Infraestructura fundamental.

SageMaker Cuotas y límites de dominios de IA

- SageMaker La SSO federación de dominios de AI Studio solo se admite en la región, en todas las cuentas de los miembros de la AWS organización en la que se aprovisiona AWS Identity Center.
- Actualmente, los espacios compartidos no son compatibles con los dominios configurados con AWS Identity Center.
- VPCy la configuración de la subred no se puede cambiar después de crear el dominio. Sin embargo, puede crear un dominio nuevo con una configuración de subred diferenteVPC.
- El acceso al dominio no se puede cambiar de un IAM SSO modo a otro después de crear el dominio. Puede crear un dominio nuevo con un modo de autenticación diferente.
- Hay un límite de cuatro aplicaciones de puerta de enlace del núcleo por tipo de instancia lanzadas para cada usuario.
- Cada usuario puede lanzar solo una instancia de cada tipo de instancia.
- Hay límites en cuanto a los recursos que se consumen en un dominio, como el número de instancias lanzadas por tipo de instancia y el número de perfiles de usuario que se pueden crear. Consulta la página de cuotas de servicio para obtener una lista completa de los límites de servicio.

- Los clientes pueden presentar un caso de soporte empresarial con una justificación empresarial para aumentar los límites de recursos predeterminados, como el número de dominios o perfiles de usuario, sujetos a restricciones a nivel de cuenta.
- El límite máximo de aplicaciones simultáneas por cuenta es de 2500 aplicaciones. Los límites de dominios y perfiles de usuario dependen de este límite estricto. Por ejemplo, una cuenta puede tener un único dominio con 1000 perfiles de usuario o 20 dominios con 50 perfiles de usuario cada uno.

Administración de identidades

En esta sección, se explica cómo los usuarios del personal de un directorio corporativo se federan en SageMaker AI Studio Cuentas de AWS y acceden a él. En primer lugar, describiremos brevemente cómo se asignan los usuarios, los grupos y los roles, y cómo funciona la federación de usuarios.

Usuarios, grupos y rol

En AWS, los permisos de los recursos se administran mediante usuarios, grupos y roles. Los clientes pueden administrar sus usuarios y grupos a través de un directorio corporativoIAM, como Active Directory (AD), habilitado a través de un IdP externo, como Okta, que les permite autenticar a los usuarios en varias aplicaciones que se ejecutan en la nube y en las instalaciones.

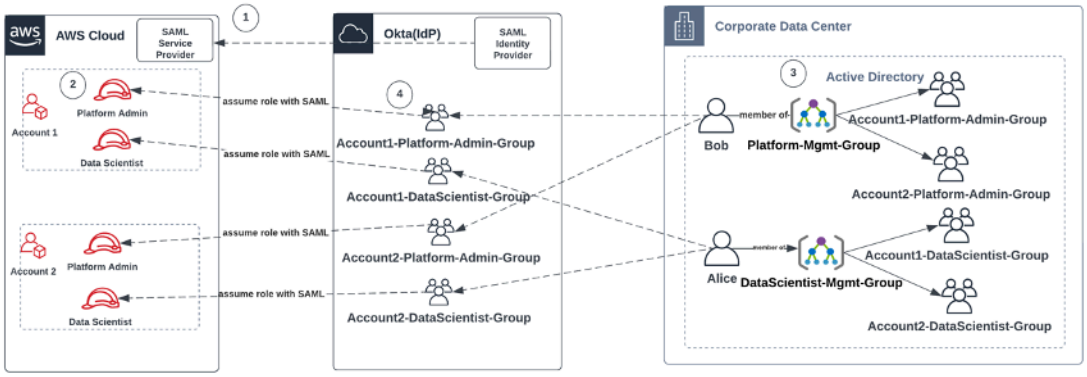
Como se explica en la sección Gestión de la identidad del pilar de AWS seguridad, se recomienda gestionar las identidades de los usuarios en un IdP central, ya que esto ayuda a integrarse fácilmente con los procesos de recursos humanos internos y ayuda a gestionar el acceso a los usuarios de su fuerza laboral.

IdPs como Okta, permiten a los usuarios finales autenticarse en uno o varios roles Cuentas de AWS y acceder a funciones específicas utilizando SSO el lenguaje de marcado de afirmaciones de seguridad (). SAML Los administradores del IdP tienen la capacidad de descargar funciones desde el Cuentas de AWS IdP y asignarlas a los usuarios. Al iniciar sesión en AWS, a los usuarios finales se les presenta una AWS pantalla en la que se muestra una lista de los AWS roles que se les han asignado en uno o varios de ellos. Cuentas de AWS Pueden seleccionar el rol que deseen asumir para el inicio de sesión, que define sus permisos durante dicha sesión autenticada.

Debe existir un grupo en el IdP para cada combinación específica de cuentas y roles a la que desee proporcionar acceso. Puede pensar en estos grupos como grupos específicos de rol de AWS . A cualquier usuario que sea miembro de estos grupos específicos de rol se le concede un único derecho: el acceso a un rol específico en una Cuenta de AWS específica. Sin embargo, este proceso de concesión de un único derecho no se escala para administrar el acceso de los usuarios mediante la asignación de cada usuario a grupos de roles de AWS específicos. Para simplificar la administración, le recomendamos que también cree varios grupos para todos los distintos conjuntos de usuarios de su organización que requieren diferentes conjuntos de AWS derechos.

Para ilustrar la configuración del IdP central, considere una empresa con una configuración de AD donde los usuarios y los grupos estén sincronizados con el directorio del IdP. En AWS, estos grupos

de AD están asignados a roles. IAM A continuación, se muestran los principales pasos del flujo de trabajo:



Flujo de trabajo para la incorporación de usuarios, grupos y roles de AD IAM

1. En AWS, configure la SAML integración de cada uno de ustedes Cuentas de AWS con su IdP.
2. En AWS, configura los roles en cada uno Cuenta de AWS y sincronízalos con el IdP.
3. En el sistema AD corporativo:
   a. Crea un grupo de AD para cada rol de cuenta y sincronízalo con el IdP (por ejemplo, `Account1-Platform-Admin-Group` (también conocido como grupo de AWS roles)).
   b. Crea un grupo de administración en cada nivel de persona (por ejemplo`Platform-Mgmt-Group`) y asigna grupos de AWS roles como miembros.
   c. Asigne usuarios a ese grupo de administración para permitir el acceso a Cuenta de AWS los roles.
4. En IdP, asigne grupos de AWS roles (como`Account1-Platform-Admin-Group`) a Cuenta de AWS roles (como Administrador de plataforma en Account1).
5. Cuando la científica de datos Alice inicia sesión en Idp, se le presenta una interfaz de usuario de AWS Federation App con dos opciones entre las que elegir: «Cuenta 1 científica de datos» y «Cuenta 2 científica de datos».
6. Alice elige la opción «Científico de datos de la cuenta 1» y se conecta a su aplicación autorizada en la cuenta 1 (AI Console). AWS SageMaker

Para obtener instrucciones detalladas sobre cómo configurar la federación de SAML cuentas, consulta Cómo configurar SAML 2.0 para la federación de cuentas de Okta. AWS

Federación de usuarios

La autenticación de SageMaker AI Studio se puede realizar mediante IAM IAM iDC. Si los usuarios se gestionan de forma IAM completa, pueden elegir el IAM modo. Si la empresa utiliza un IdP externo, puede federarse a través IAM de un IdC. IAM Ten en cuenta que el modo de autenticación no se puede actualizar para un dominio de SageMaker AI Studio existente, por lo que es fundamental tomar la decisión antes de crear un dominio de SageMaker AI Studio de producción.

Si SageMaker AI Studio está configurado en IAM modo, los usuarios de SageMaker AI Studio acceden a la aplicación a través de un dispositivo prefirmado URL que inicia sesión automáticamente en la aplicación de SageMaker AI Studio cuando se accede a ella a través de un navegador.

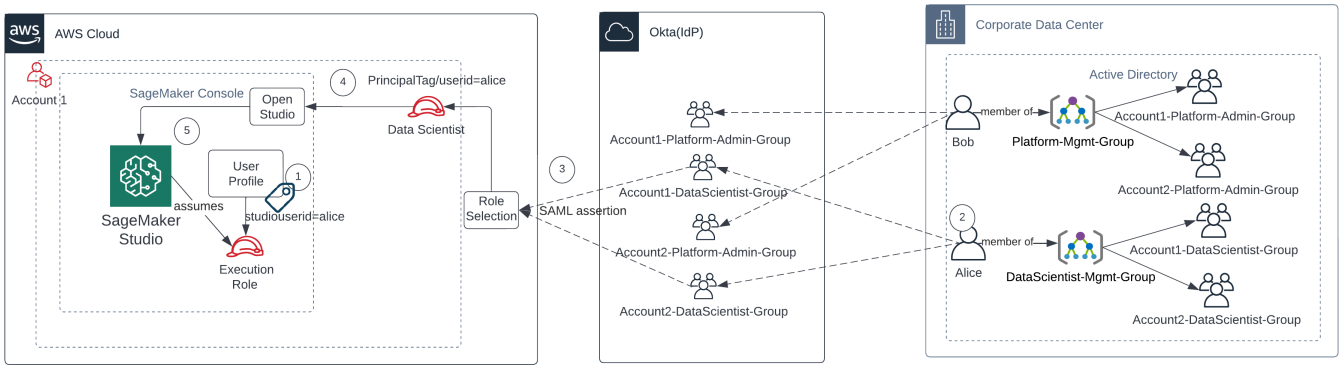
Usuarios de IAM

Para IAM los usuarios, el administrador crea perfiles de usuario de SageMaker AI Studio para cada usuario y asocia el perfil de usuario a un IAM rol que permite realizar las acciones necesarias que el usuario debe realizar desde Studio. Para impedir que un AWS usuario acceda únicamente a su perfil de usuario de SageMaker AI Studio, el administrador debe etiquetar el perfil de usuario de SageMaker AI Studio y adjuntar una IAM política al usuario que le permita acceder solo si el valor de la etiqueta es el mismo que el nombre de AWS usuario. La declaración de política es similar a la siguiente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonSageMakerPresignedUrlPolicy",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "sagemaker:ResourceTag/studiouserid": "${aws:username}"
                }
            }
        }
    ]
}
```

AWS IAMo federación de cuentas

El método de Cuenta de AWS federación permite a los clientes federarse en la consola de SageMaker IA desde su SAML IdP, como Okta. Para impedir que los usuarios accedan únicamente a su perfil de usuario, el administrador debe etiquetar el perfil de usuario de SageMaker AI Studio, añadir `PrincipalTags` el IdP y configurarlo como etiquetas transitivas. El siguiente diagrama muestra cómo el usuario federado (Alice, la científica de datos) está autorizado a acceder a su propio perfil de usuario de SageMaker AI Studio.



Acceder a SageMaker AI Studio en IAM modo de federación

1. El perfil de usuario de Alice SageMaker AI Studio está etiquetado con su ID de usuario y asociado a la función de ejecución.
2. Alice se autentica en el IdP (Okta).
3. El IdP autentica a Alice y publica una SAML afirmación con las dos funciones (científica de datos para las cuentas 1 y 2) de las que es miembro Alice. Alice selecciona el rol Científico de datos para la cuenta 1.
4. Alice ha iniciado sesión en la consola de SageMaker IA de la cuenta 1 y ha asumido el rol de científica de datos. Alice abre su instancia de aplicación de Studio desde la lista de instancias de aplicaciones de Studio.
5. La etiqueta principal de Alice en la sesión de rol asumida se valida con la etiqueta de perfil de usuario de la instancia de aplicación de SageMaker AI Studio seleccionada. Si la etiqueta de perfil es válida, se lanza la instancia de la aplicación SageMaker AI Studio y asume la función de ejecución.

Si quieres automatizar la creación de roles y políticas de ejecución de SageMaker IA como parte de la incorporación de usuarios, puedes hacerlo de la siguiente manera:

1. Configure un grupo de AD, por ejemplo, `SageMaker AI-Account1-Group` en cada nivel de cuenta y dominio de Studio.
2. Añade SageMaker AI-Account1-Group a la membresía del grupo de usuarios cuando necesites incorporar a un usuario a AI Studio. SageMaker

Configura un proceso de automatización que escuche el evento de `SageMaker AI-Account1-Group` membresía y utilízalo AWS APIs para crear el rol, las políticas, las etiquetas y el perfil de usuario de SageMaker AI Studio en función de sus miembros al grupo de AD. Asocie el rol con el perfil de usuario. Para ver un ejemplo de política, consulta. Impida que los usuarios de SageMaker AI Studio accedan a otros perfiles de usuario

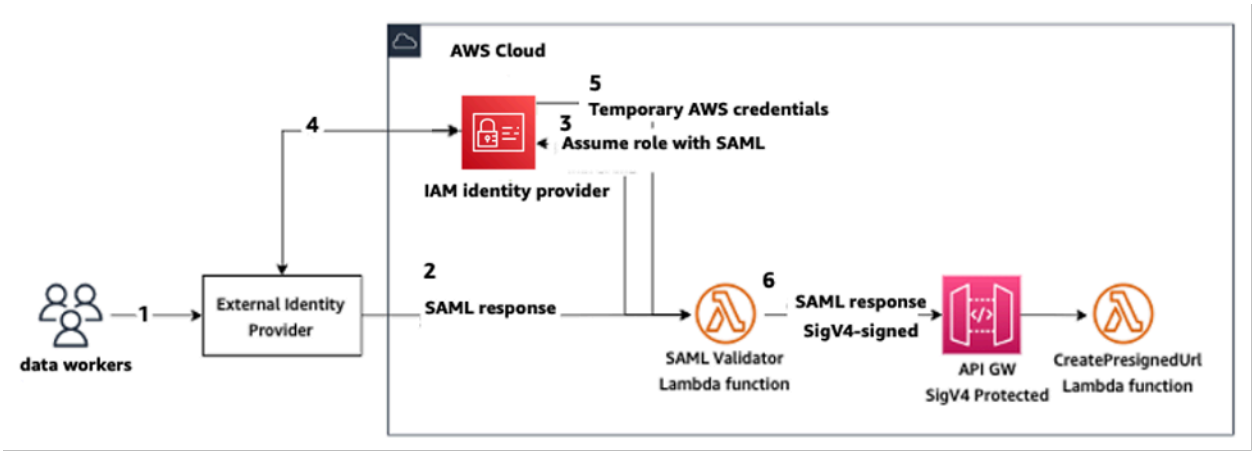
SAMLautenticación mediante AWS Lambda

En IAM este modo, los usuarios también pueden autenticarse en SageMaker AI Studio mediante SAML aserciones. En esta arquitectura, el cliente tiene un IdP existente, donde puede crear una SAML aplicación para que los usuarios accedan a Studio (en lugar de a la aplicación AWS Identity Federation). Se añade el IdP del cliente a. IAM Una AWS Lambda función ayuda a validar la SAML afirmación mediante IAM ySTS, a continuación, invoca directamente una API puerta de enlace o una función Lambda para crear el dominio prefirmado. URL

La ventaja de esta solución es que la función Lambda puede personalizar la lógica para acceder a SageMaker AI Studio. Por ejemplo:

- Cree automáticamente un perfil de usuario si no existe uno.
- Adjunte o elimine funciones o documentos de políticas a la función de ejecución de SageMaker AI Studio analizando los SAML atributos.
- Personalice el perfil de usuario añadiendo la configuración del ciclo de vida (LCC) y añadiendo etiquetas.

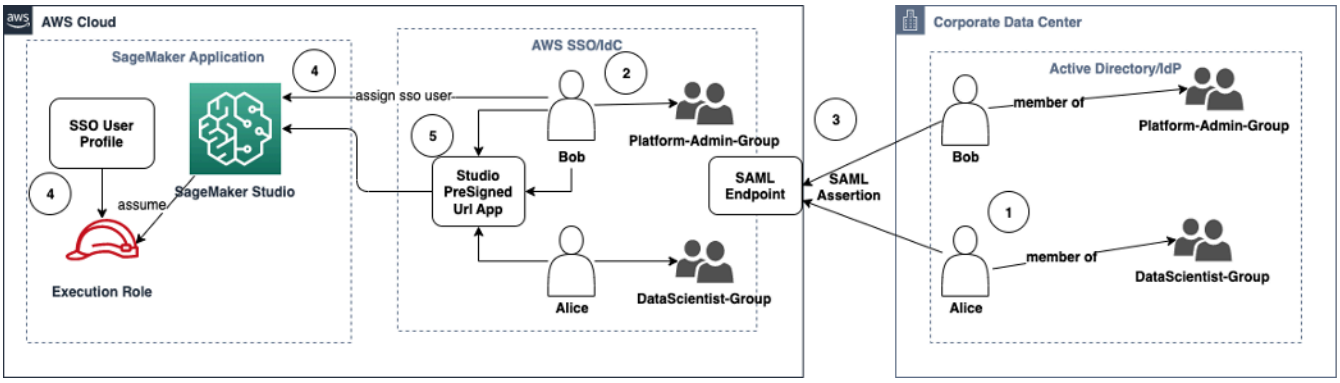
En resumen, esta solución mostrará SageMaker AI Studio como una aplicación SAML2 4.0 con una lógica personalizada para la autenticación y la autorización. Consulte la sección del apéndice Acceso a SageMaker Studio mediante SAML aserción para obtener detalles sobre la implementación.



Acceder a SageMaker AI Studio mediante una SAML aplicación personalizada

AWSIAMFederación iDC

El método de federación iDC permite a los clientes federarse directamente en la aplicación SageMaker AI Studio desde su SAML IdP (como Okta). En el siguiente diagrama, se muestra cómo el usuario federado está autorizado a acceder a su propia instancia de AI Studio. SageMaker



Acceder a SageMaker AI Studio en modo IAM iDC

1. En el AD corporativo, el usuario es miembro de grupos de AD como, por ejemplo, el grupo Administrador de plataforma y el grupo Científico de datos.
2. El usuario de AD y los grupos de AD del proveedor de identidad (IdP) se sincronizan con AWS IAM Identity Center y están disponibles como usuarios y grupos de inicio de sesión único para las asignaciones, respectivamente.
3. El IdP publica una SAML afirmación en el punto final del AWS iDC. SAML
4. En SageMaker AI Studio, el usuario de iDC está asignado a la aplicación Studio. SageMaker Esta tarea se puede realizar mediante iDC Group y SageMaker AI Studio se aplicará a cada nivel de

usuario de iDC. Cuando se crea esta asignación, SageMaker AI Studio crea el perfil de usuario de iDC y asigna la función de ejecución del dominio.

5. El usuario accede a la aplicación SageMaker AI Studio mediante la aplicación segura y prefirmada URL alojada como una aplicación en la nube desde el iDC. SageMaker AI Studio asume la función de ejecución asociada a su perfil de usuario de iDC.

Guía de autenticación de dominios

Estas son algunas consideraciones a tener en cuenta cuando se elige el modo de autenticación de un dominio:

1. Si quieres que tus usuarios no accedan a la AWS Management Console interfaz de usuario de SageMaker AI Studio ni la vean directamente, utiliza el modo de inicio de sesión único con iDC. AWS IAM
2. Si quieres que tus usuarios no accedan a la AWS Management Console interfaz de usuario de SageMaker AI Studio ni la vean directamente en el IAM modo, puedes hacerlo mediante una función Lambda en el backend URL para generar un perfil de usuario prefirmado y redirigirlos a la interfaz de usuario de AI Studio. SageMaker
3. En el modo IdC, cada usuario se asigna a un único perfil de usuario.
4. A todos los perfiles de usuario se les asigna automáticamente el rol de ejecución predeterminado en modo IdC. Si quieres que a tus usuarios se les asignen diferentes funciones de ejecución, tendrás que actualizar los perfiles de usuario mediante el. UpdateUserProfileAPI
5. Si quieres restringir el acceso a la interfaz de usuario de SageMaker AI Studio en IAM modo (con el prefirmado generadoURL) a un VPC terminal, sin tener que atravesar Internet, puedes usar un solucionador personalizado. DNS Consulte la entrada del blog prefirmada Secure Amazon SageMaker AI Studio URLs Part 1: Foundational Infrastructure.

Administración de permisos

En esta sección se analizan las mejores prácticas para configurar las IAM funciones, políticas y barreras de protección más utilizadas para el aprovisionamiento y el funcionamiento del dominio de AI Studio. SageMaker

Roles y políticas de IAM

Como práctica recomendada, tal vez quieras identificar primero a las personas y aplicaciones relevantes, conocidas como responsables, que participan en el ciclo de vida del aprendizaje automático, y qué AWS permisos necesitas concederles. Como la SageMaker IA es un servicio gestionado, también hay que tener en cuenta los principios de servicio, que son AWS servicios que pueden realizar API llamadas en nombre de un usuario. El siguiente diagrama ilustra los diferentes IAM roles que puede querer crear, correspondientes a las distintas personas de la organización.

SageMaker IAMFunciones de IA

Estas funciones se describen en detalle, junto con algunos ejemplos específicos IAMpermissions que necesitarán.

- Función de usuario de ML Admin: se trata de un director que proporciona el entorno a los científicos de datos mediante la creación de dominios y perfiles de usuario de estudio (`sagemaker:CreateDomain`,`sagemaker:CreateUserProfile`), la creación de claves AWS Key Management Service (AWS KMS) para los usuarios, la creación de depósitos de S3 para los científicos de datos y la creación de ECR repositorios de Amazon para alojar contenedores. También pueden establecer configuraciones y scripts de ciclo de vida predeterminados para los usuarios, crear y adjuntar imágenes personalizadas al dominio de SageMaker AI Studio y proporcionar productos de Service Catalog, como proyectos personalizados y EMR plantillas de Amazon.

  Como este director no realizará tareas de formación, por ejemplo, no necesitará permisos para iniciar tareas de formación o procesamiento de SageMaker IA. Si utilizan la infraestructura como

plantillas de código, como CloudFormation Terraform, para aprovisionar dominios y usuarios, el servicio de aprovisionamiento asumiría esta función para crear los recursos en nombre del administrador. Esta función puede tener acceso de solo lectura a la IA mediante el SageMaker . AWS Management Console

Esta función de usuario también necesitará ciertos EC2 permisos para lanzar el dominio dentro de una cuenta privadaVPC, KMS permisos para cifrar el EFS volumen y permisos para crear una función vinculada a un servicio para Studio (). `iam:CreateServiceLinkedRole` Describiremos esos permisos detallados más adelante en el documento.

- Función de usuario del científico de datos: el principal consiste en que el usuario inicie sesión en SageMaker AI Studio, explore los datos, cree tareas y procesos de procesamiento y formación, etc. El permiso principal que necesita el usuario es el permiso para iniciar SageMaker AI Studio, y el resto de las políticas las puede gestionar el rol de servicio de ejecución de SageMaker IA.
- SageMaker Función de servicio de ejecución de SageMaker IA: dado que la IA es un servicio gestionado, lanza trabajos en nombre del usuario. Esta función suele ser la más amplia en términos de permisos permitidos, ya que muchos clientes optan por utilizar una única función de ejecución para ejecutar tareas de formación, tareas de procesamiento o modelar tareas de hospedaje. Si bien esta es una forma fácil de empezar, dado que los clientes maduran a medida que avanzan, suelen dividir la función de ejecución del portátil en funciones independientes para distintas API acciones, especialmente cuando ejecutan esas tareas en entornos implementados.

  Al crearlo, asocias un rol al dominio de SageMaker AI Studio. Sin embargo, dado que los clientes pueden necesitar la flexibilidad de tener diferentes funciones asociadas a los distintos perfiles de usuario del dominio (por ejemplo, en función de su función laboral), también puedes asociar una IAM función independiente a cada perfil de usuario. Se recomienda asignar un único usuario físico a un único perfil de usuario. Si no adjuntas un rol a un perfil de usuario al crearlo, el comportamiento predeterminado es asociar también el rol de ejecución del SageMaker AIStudio dominio al perfil de usuario.

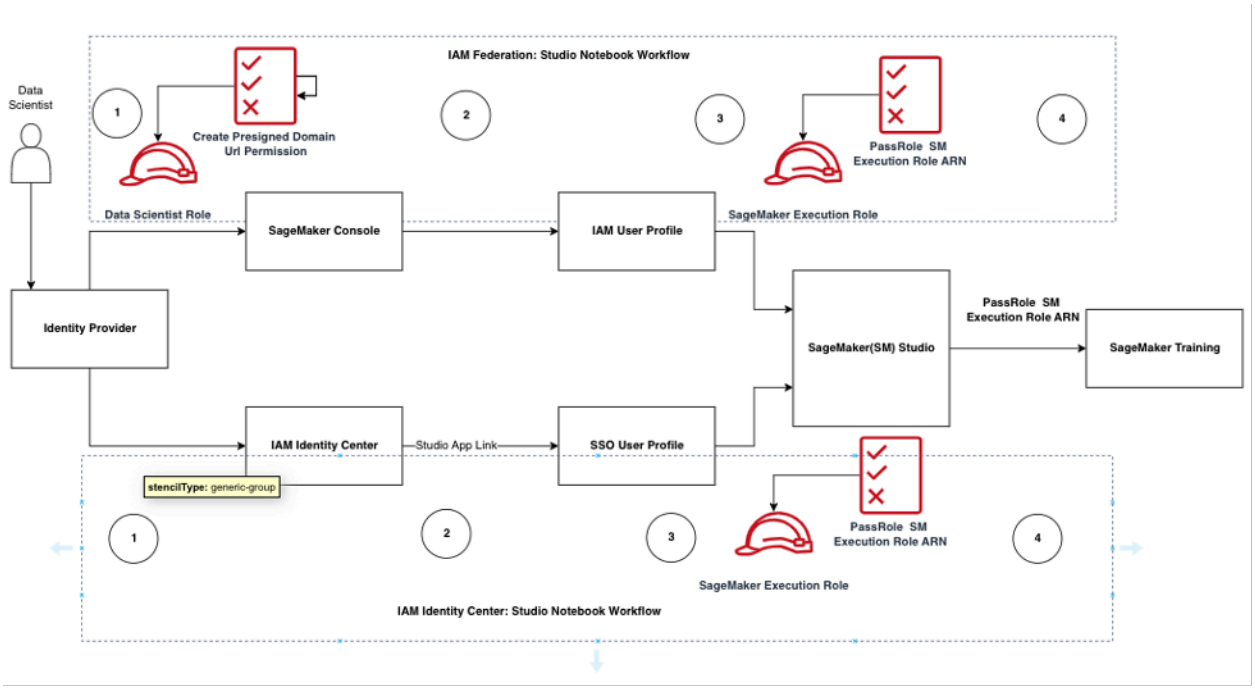
  En los casos en que varios científicos de datos e ingenieros de aprendizaje automático trabajen juntos en un proyecto y necesiten un modelo de permisos compartido para acceder a los recursos, le recomendamos que cree una función de ejecución de servicios de SageMaker IA a nivel de equipo para compartir IAM los permisos entre los miembros de su equipo. En los casos en los que necesites bloquear los permisos en cada nivel de usuario, puedes crear un rol individual de ejecución de servicios de SageMaker IA a nivel de usuario; sin embargo, debes tener en cuenta tus límites de servicio.

SageMaker Proceso de autorización de AI Studio Notebook

En esta sección, se explica cómo funciona la autorización de SageMaker AI Studio Notebook para diversas actividades que el científico de datos debe realizar para crear y entrenar el modelo directamente desde SageMaker AI Studio Notebook. El dominio SageMaker AI admite dos modos de autorización:

- IAMfederación
- IAMCentro de identidad

A continuación, este paper explica el flujo de trabajo de autorización de Data Scientist para cada uno de esos modos.



Flujo de trabajo de autenticación y autorización para usuarios de Studio

IAMFederación: flujos de trabajo de SageMaker Studio Notebook

1. Un científico de datos se autentica en su proveedor de identidad corporativa y asume el rol de usuario de científico de datos (el rol de federación de usuarios) en la consola de SageMaker IA. Esta función de federación tiene `iam:PassRole` API permiso en la función de ejecución de SageMaker IA para transferir la función Amazon Resource Name (ARN) a SageMaker Studio.

2. El científico de datos selecciona el enlace de Open Studio de su perfil de IAM usuario de Studio que está asociado a la función de ejecución de la SageMaker IA
3. Se inicia el IDE servicio SageMaker Studio, siempre que los permisos de la función de SageMaker ejecución del perfil de usuario estén habilitados. Esta función tiene `iam:PassRole` API permiso sobre la función de ejecución de SageMaker IA para transferirla ARN al servicio de formación de SageMaker IA.
4. Cuando el científico de datos inicia la tarea de formación en los nodos de computación remotos, la función de ejecución de la SageMaker IA ARN pasa al servicio de formación de la SageMaker IA. De este modo, se crea una nueva sesión de rol ARN y se ejecuta el trabajo de formación. Si necesitas ampliar aún más el permiso para un puesto de formación, puedes crear un puesto de formación específico y transferirlo ARN al solicitar un puesto de formaciónAPI.

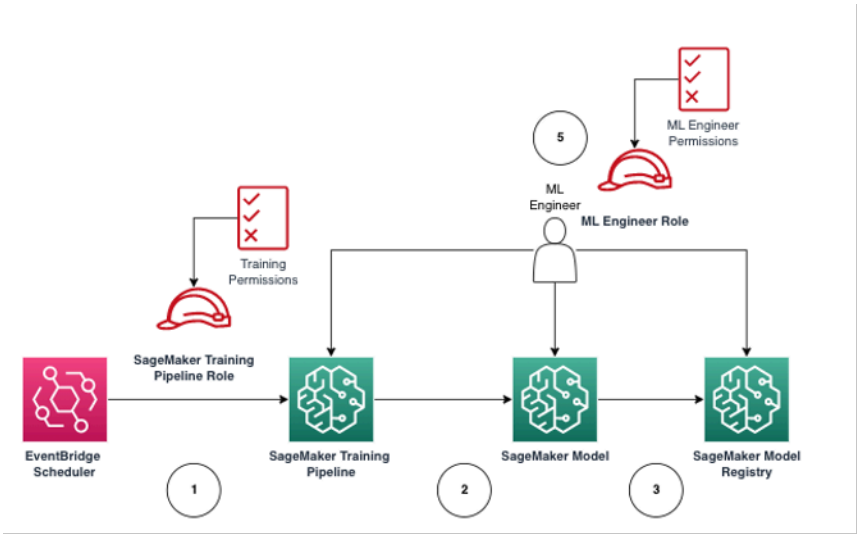
IAMIdentity Center: flujo de trabajo de SageMaker AI Studio Notebook

1. El científico de datos se autentica en su proveedor de identidad corporativa y hace clic en AWS IAM Identity Center. Al científico de datos se le presenta el portal Identity Center para el usuario.
2. El científico de datos hace clic en el enlace de la aplicación SageMaker AI Studio que se creó a partir de su perfil de usuario de iDC, que está asociado a la función de ejecución de la SageMaker IA.
3. Se inicia el IDE servicio SageMaker AI Studio, siempre y cuando los permisos de la función de ejecución de SageMaker IA del perfil de usuario estén habilitados. Esta función tiene `iam:PassRole` API permiso sobre la función de ejecución de SageMaker IA para transferirla ARN al servicio de formación de SageMaker IA.
4. Cuando el científico de datos inicia la tarea de formación en los nodos de computación remotos, la función de ejecución de la SageMaker IA ARN pasa al servicio de formación de la SageMaker IA. El rol de ejecución ARN crea una nueva sesión de rol con esto ARN y ejecuta el trabajo de capacitación. Si necesita limitar aún más el permiso para los trabajos de formación, puede crear un puesto específico para la formación y transferirlo ARN cuando convoque la formación. API

Entorno implementado: flujo de trabajo de formación en SageMaker IA

En los entornos implementados, como las pruebas de sistemas y la producción, los trabajos se ejecutan mediante un programador automático y activadores de eventos, y el acceso humano a esos entornos está restringido desde los cuadernos de SageMaker AI Studio. En esta sección, se explica

cómo funcionan IAM las funciones con el proceso de formación en SageMaker IA en el entorno desplegado.



SageMaker Flujo de trabajo de formación en IA en un entorno de producción gestionado

1. El EventBridge programador de Amazon activa el proceso de formación de SageMaker IA.
2. El SageMaker trabajo del proceso de formación en SageMaker IA asume la función del proceso de formación en IA para capacitar al modelo.
3. El modelo de SageMaker IA entrenado está registrado en el Registro de modelos de SageMaker IA.
4. Un ingeniero de aprendizaje automático asume la función de usuario de ingeniero de aprendizaje automático para gestionar el proceso de formación y el modelo de SageMaker IA.

Permisos para los datos

La capacidad de los usuarios de SageMaker AI Studio de acceder a cualquier fuente de datos depende de los permisos asociados a su función de IAM ejecución de la SageMaker IA. Las políticas adjuntas pueden autorizarles a leer, escribir o eliminar determinados buckets o prefijos de Amazon S3 y a conectarse a las bases de datos de AmazonRDS.

Acceder a los datos AWS Lake Formation

Muchas empresas han empezado a utilizar lagos de datos AWS Lake Formationque permiten a sus usuarios un acceso detallado a los datos. Como ejemplo de este tipo de datos gobernados, los

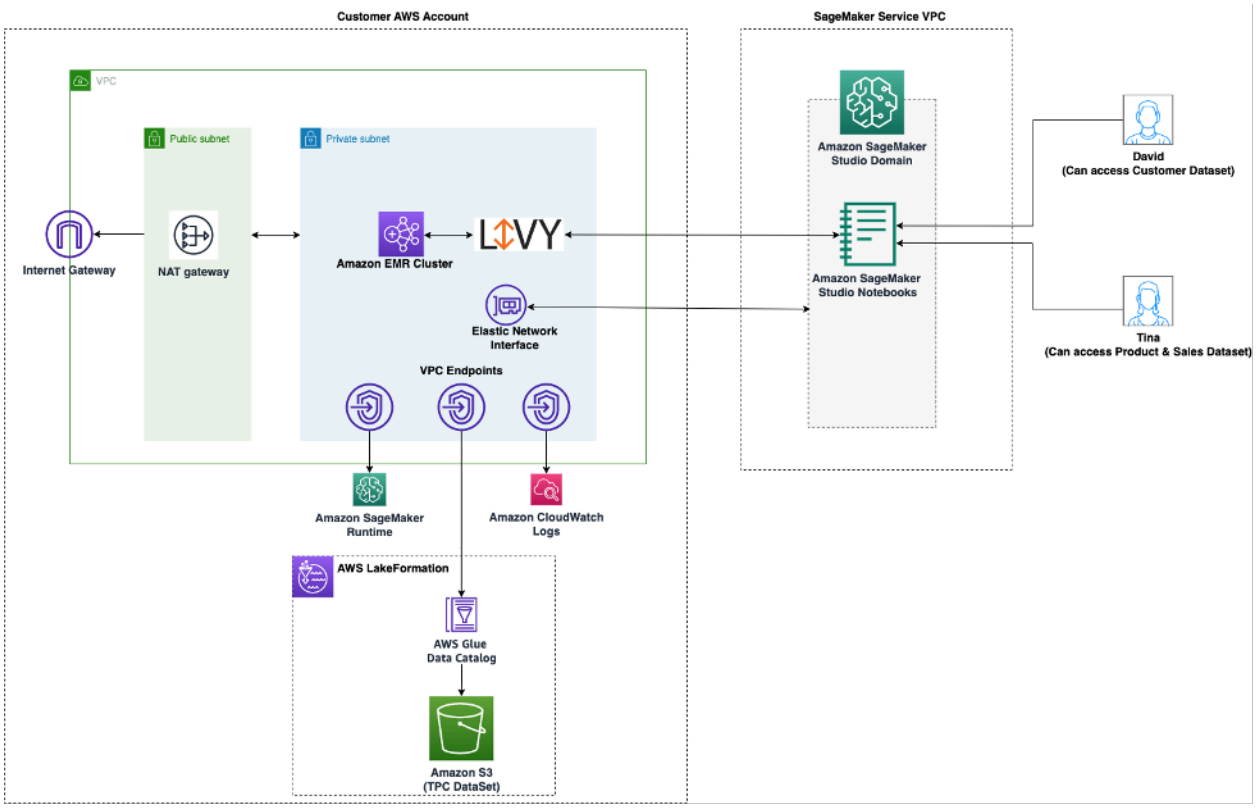
administradores pueden ocultar columnas confidenciales para algunos usuarios y, al mismo tiempo, habilitar las consultas de la misma tabla subyacente.

Para utilizar Lake Formation de SageMaker AI Studio, los administradores pueden registrar las funciones de IAM ejecución de SageMaker IA como`DataLakePrincipals`. Para obtener más información, consulte Referencia de permisos de Lake Formation. Una vez autorizados, hay tres métodos principales para acceder a los datos gobernados desde SageMaker AI Studio y escribirlos:

1. Desde un cuaderno de SageMaker AI Studio, los usuarios pueden utilizar motores de consulta como Amazon Athena o bibliotecas que se basan en boto3 para extraer datos directamente al cuaderno. La biblioteca AWSSDKfor Pandas (anteriormente conocida como awswrangler) es una biblioteca popular. El siguiente es un ejemplo de código para mostrar lo sencillo que puede ser:

```
transaction_id = wr.lakeformation.start_transaction(read_only=True)
df = wr.lakeformation.read_sql_query(
    sql=f"SELECT * FROM {table};",
    database=database,
    transaction_id=transaction_id
)
```

2. Usa la conectividad nativa de SageMaker AI Studio con Amazon EMR para leer y escribir datos a escala. Mediante el uso de las funciones de EMR ejecución de Apache Livy y Amazon, SageMaker AI Studio ha creado una conectividad nativa que le permite transferir su función de ejecución de SageMaker IA (u otra IAM función autorizada) a un EMR clúster de Amazon para acceder a los datos y procesarlos. Consulta Connect to an Amazon EMR Cluster from Studio para up-to-date obtener instrucciones.



Arquitectura para acceder a los datos gestionados por Lake Formation desde SageMaker Studio

3. Utilice la conectividad nativa de SageMaker AI Studio en sesiones AWS Glue interactivas para leer y escribir datos a escala. SageMaker Los cuadernos de AI Studio tienen núcleos integrados que permiten a los usuarios ejecutar comandos de forma interactiva. AWS Glue Esto permite el uso escalable de los backends de Python, Spark o Ray, que pueden leer y escribir datos a escala sin problemas desde fuentes de datos gobernadas. Los núcleos permiten a los usuarios transferir sus funciones de SageMaker ejecución u otras funciones autorizadasIAM. Consulte Preparar datos mediante sesiones AWS Glue interactivas para obtener más información.

Barandillas comunes

En esta sección, se analizan las barreras de protección más utilizadas para controlar los recursos de aprendizaje automático mediante IAM políticas, políticas de recursos, políticas de VPC puntos finales y políticas de control de servicios (). SCPs

Limite el acceso de las computadoras portátiles a instancias específicas

Esta política de control de servicios se puede utilizar para limitar los tipos de instancias a los que tienen acceso los científicos de datos al crear libretas de Studio. Ten en cuenta que cualquier usuario

necesitará que la instancia del «sistema» esté habilitada para crear la aplicación predeterminada de Jupyter Server que aloja SageMaker AI Studio.

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "LimitInstanceTypesforNotebooks",
             "Effect": "Deny",
             "Action": [
                 "sagemaker:CreateApp"
             ],
             "Resource": "*",
             "Condition": {
                 "ForAnyValue:StringNotLike": {
                     "sagemaker:InstanceTypes": [
                         "ml.c5.large",
                         "ml.m5.large",
                         "ml.t3.medium",
                         "system"
                     ]
                 }
             }
         }
     ]
 }
```

Limita los dominios de AI Studio que no cumplan con los requisitos SageMaker

En el caso de los dominios de SageMaker AI Studio, se puede utilizar la siguiente política de control de servicios para hacer que el tráfico acceda a los recursos de los clientes, de modo que no pase por la Internet pública, sino por la de VPC un cliente:

```
{
     "Version": "2012-10-17",
     "Statement": [
         {   "Sid": "LockDownStudioDomain",
             "Effect": "Deny",
             "Action": [
                 "sagemaker:CreateDomain"
```

```
            ],
            "Resource": "*",
            "Condition": {
                        "StringNotEquals": {"sagemaker:AppNetworkAccessType":
"VpcOnly"
                },
                "Null": {
                        "sagemaker:VpcSubnets": "true",
                        "sagemaker:VpcSecurityGroupIds": "true"
                }
            }
        }
    ]
}
```

Limite el lanzamiento de imágenes de SageMaker IA no autorizadas

La siguiente política impide que un usuario lance una imagen de SageMaker IA no autorizada dentro de su dominio:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "sagemaker:CreateApp"
             ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringNotLike": {
                    "sagemaker:ImageArns":
                        [
                        "arn:aws:sagemaker:*:*:image/{ImageName}"
                        ]
                }
            }
        }
    ]
}
```

Lance blocs de notas únicamente a través de terminales de IA SageMaker VPC

Además de los VPC puntos finales del plano de control de la IA, SageMaker la SageMaker IA admite VPC puntos finales para que los usuarios se conecten a las libretas de SageMaker AI Studio o a las instancias de las libretas de IA. SageMaker Si ya has configurado un VPC punto final para una instancia de SageMaker AI Studio/Notebook, la siguiente clave de IAM condición solo permitirá las conexiones a los cuadernos de SageMaker AI Studio si se realizan a través del punto final de SageMaker AI Studio o del VPC punto final de IA. SageMaker API

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Sid": "EnableSageMakerStudioAccessviaVPCEndpoint",
             "Effect": "Allow",
             "Action": [
                 "sagemaker:CreatePresignedDomainUrl",
                 "sagemaker:DescribeUserProfile"
             ],
             "Resource": "*",
             "Condition": {
                 "ForAnyValue:StringEquals": {
                     "aws:sourceVpce": [
                         "vpce-111bbccc",
                         "vpce-111bbddd"
                     ]
                 }
             }
         }
     ]
 }
```

Limita el acceso al portátil SageMaker AI Studio a un rango de IP limitado

Las empresas suelen limitar el acceso a SageMaker AI Studio a ciertos rangos de IP corporativos permitidos. La siguiente IAM política con la clave de `SourceIP` condición puede limitar esta situación.

```
{
     "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "EnableSageMakerStudioAccess",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl",
                "sagemaker:DescribeUserProfile"
            ],
            "Resource": "*",
            "Condition": {
                "IpAddress": {
                    "aws:SourceIp": [
                        "192.0.2.0/24",
                        "203.0.113.0/24"
                    ]
                }
            }
        }
    ]
}
```

Impida que los usuarios de SageMaker AI Studio accedan a otros perfiles de usuario

Como administrador, al crear el perfil de usuario, asegúrate de que el perfil esté etiquetado con el nombre de usuario de SageMaker AI Studio con la clave de la etiqueta`studiouserid`. El principal (usuario o rol asociado al usuario) también debe tener una etiqueta con la clave `studiouserid` (esta etiqueta puede tener cualquier nombre y no se limita a él`studiouserid`).

A continuación, adjunte la siguiente política a la función que asumirá el usuario al lanzar SageMaker AI Studio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AmazonSageMakerPresignedUrlPolicy",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreatePresignedDomainUrl"
            ],
            "Resource": "*",
```

```
            "Condition": {
                "StringEquals": {
                    "sagemaker:ResourceTag/studiouserid": "${aws:PrincipalTag/
studiouserid}"
                }
            }
        }
    ]
}
```

Imponga el etiquetado

Los científicos de datos necesitan usar los cuadernos de SageMaker AI Studio para explorar los datos y crear y entrenar modelos. Aplicar etiquetas a las libretas ayuda a supervisar el uso y controlar los costes, además de garantizar la propiedad y la auditabilidad.

En el caso de las aplicaciones de SageMaker AI Studio, asegúrate de que el perfil de usuario esté etiquetado. Las etiquetas se propagan automáticamente a las aplicaciones desde el perfil de usuario. Para forzar la creación de perfiles de usuario con etiquetas (se admite mediante CLI ySDK), considere la posibilidad de añadir esta política a la función de administrador:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceUserProfileTags",
            "Effect": "Allow",
            "Action": "sagemaker:CreateUserProfile",
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "studiouserid"
                    ]
                }
            }
        }
    ]
}
```

Para otros recursos, como los trabajos de formación y los trabajos de procesamiento, puedes hacer que las etiquetas sean obligatorias mediante la siguiente política:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnforceTagsForJobs",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateTrainingJob",
                "sagemaker:CreateProcessingJob",
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:TagKeys": [
                        "studiouserid"
                    ]
                }
            }
        }
    ]
}
```

Acceso root en SageMaker AI Studio

En SageMaker AI Studio, el bloc de notas se ejecuta en un contenedor de Docker que, de forma predeterminada, no tiene acceso root a la instancia host. Del mismo modo, excepto el usuario en ejecución predeterminado, todos los demás rangos de ID de usuario del contenedor se reasignan como usuarios sin privilegios en la propia instancia host. IDs Como resultado, la amenaza de una escalada de privilegios se limita al propio contenedor del portátil.

Al crear imágenes personalizadas, es posible que desee proporcionar a su usuario permisos distintos de los de root para poder aplicar controles más estrictos; por ejemplo, evitar ejecutar procesos no deseados como root o instalar paquetes disponibles públicamente. En esos casos, puedes crear la imagen para que se ejecute como usuario no root en el Dockerfile. Tanto si creas el usuario como root como si no, debes asegurarte de que se trata de la UID/GID of the user is identical to the UID/GID aplicación personalizada, que crea la configuración para que SageMaker AI ejecute una aplicación con la imagen personalizada. AppImageConfig Por ejemplo, si tu Dockerfile está creado para un usuario que no es root, como el siguiente:

```
ARG NB_UID="1000"
```

```
ARG NB_GID="100"
...
USER $NB_UID
```

El `AppImageConfig` archivo debe mencionar lo mismo UID y GID en su: `KernelGatewayConfig`

```
{
    "KernelGatewayImageConfig": {
        "FileSystemConfig": {
            "DefaultUid": 1000,
            "DefaultGid": 100
        }
    }
}
```

Los GID valoresUID/aceptables para las imágenes personalizadas son 0/0 y 1000/100 para las imágenes de Studio. Para ver ejemplos de creación de imágenes personalizadas y la `AppImageConfig` configuración asociada, consulta este repositorio de Github.

Para evitar que los usuarios alteren esta información, no concedas ni `DeleteAppImageConfig` permisos a los usuarios de ordenadores portátiles de SageMaker AI Studio. `CreateAppImageConfig` `UpdateAppImageConfig`

Administración de red

Para configurar el dominio de SageMaker AI Studio, debe especificar la VPC red, las subredes y los grupos de seguridad. Al especificar las subredes VPC y, asegúrate de asignarlas IPs teniendo en cuenta el volumen de uso y el crecimiento esperado, tal como se explica en las siguientes secciones.

VPCplanificación de la red

VPCLas subredes de los clientes asociadas al dominio de SageMaker AI Studio deben crearse con el rango de enrutamiento entre dominios (CIDR) sin clase adecuado, en función de los siguientes factores:

- Número de usuarios.
- Número de aplicaciones por usuario.
- Número de tipos de instancias únicos por usuario.
- Número medio de instancias de formación por usuario.
- Porcentaje de crecimiento esperado.

SageMaker La IA y AWS los servicios participantes inyectan interfaces de red elásticas (ENI) en la VPC subred del cliente para los siguientes casos de uso:

- Amazon EFS inyecta un objetivo de EFS montaje ENI para el dominio de SageMaker IA (una IP por subred/zona de disponibilidad adjunta al dominio de SageMaker IA).
- SageMaker AI Studio inyecta una ENI para cada instancia única utilizada por un perfil de usuario o un espacio compartido. Por ejemplo:
  - Si un perfil de usuario ejecuta una aplicación de servidor Jupyter predeterminada (una instancia de «sistema»), una aplicación de ciencia de datos y una aplicación Python base (ambas ejecutadas en una `ml.t3.medium` instancia), Studio inyecta dos direcciones IP.
  - Si un perfil de usuario ejecuta una aplicación de servidor Jupyter predeterminada (una instancia de «sistema»), una GPU aplicación de Tensorflow (en una `ml.g4dn.xlarge` instancia) y una aplicación de almacenamiento de datos (en una `ml.m5.4xlarge` instancia), Studio inyecta tres direcciones IP.
- Se inserta una ENI para cada VPC punto final en las VPC subredes o zonas de disponibilidad del dominio (cuatro IPs para los puntos de enlace de SageMaker IA; aproximadamente seis IPs para los VPC puntos de enlace de los servicios participantes, como S3, y.) VPC ECR CloudWatch

- Si los trabajos de formación y procesamiento de SageMaker IA se lanzan con la misma VPC configuración, cada trabajo necesita dos direcciones IP por instancia.

> **Note**
>
> VPClos ajustes de SageMaker AI Studio, como las subredes y el tráfico VPC exclusivo, no se transfieren automáticamente a los trabajos de formación o procesamiento creados desde AI Studio. SageMaker El usuario debe configurar los VPC ajustes y el aislamiento de la red según sea necesario al llamar a APIs Create*Job. Consulte Ejecutar los contenedores de entrenamiento e inferencia en modo con acceso a Internet para obtener más información.

Escenario: un científico de datos realiza experimentos en dos tipos de instancias diferentes

En este escenario, supongamos que un dominio de SageMaker IA está configurado en modo VPC de tráfico exclusivo. Hay VPC puntos de conexión configurados, como SageMaker AIAPI, SageMaker AI Runtime, Amazon S3 y AmazonECR.

Un científico de datos realiza experimentos en cuadernos de Studio, los ejecuta en dos tipos de instancias diferentes (por ejemplo, `ml.t3.medium` y`ml.m5.large`) y lanza dos aplicaciones en cada tipo de instancia.

Supongamos que el científico de datos también ejecuta simultáneamente un trabajo de formación con la misma VPC configuración en una `ml.m5.4xlarge` instancia.

En este escenario, el servicio SageMaker AI Studio se inyectará de la ENIs siguiente manera:

Tabla 1: ENIs inyectado en el cliente VPC para un escenario de experimentación

Entidad	Destino	ENIinyectado	Notas	Nivel
EFSmontar objetivo	VPCsubredes	Tres	Tres /subredes AZs	Dominio
Puntos de conexión de VPC	VPCsubredes	30	Tres AZs subredes /con 10 cada una VPCE	Dominio

Entidad	Destino	ENIinyectado	Notas	Nivel
Servidor Jupyter	Subred de VPC	Uno	Una IP por instancia	Usuario
Aplicación KernelGateway	Subred de VPC	Dos	Una IP por tipo de instancia	Usuario
Formación	Subred de VPC	Dos	Dos IPs por instancia de entrenamiento Cinco IPs por instancia de entrenamiento si EFAse utiliza	Usuario

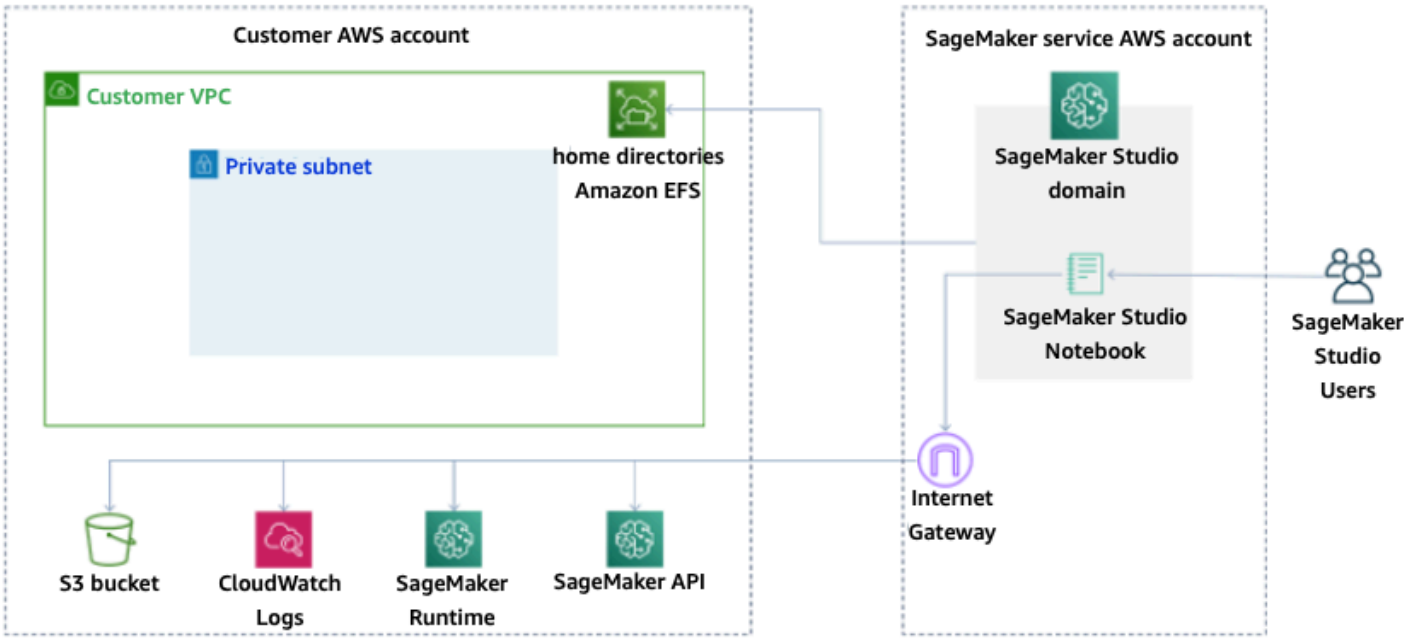
En este escenario, el cliente IPs consume un total de 38, de los VPC cuales 33 IPs se comparten entre los usuarios a nivel de dominio y cinco IPs se consumen a nivel de usuario. Si tiene 100 usuarios con perfiles de usuario similares en este dominio que realizan estas actividades simultáneamente, consumirá cinco x 100 = 500 IPs a nivel de usuario, además del consumo de IP a nivel de dominio, que es de 11 IPs por subred, lo que arroja un total de 511. IPs Para este escenario, debe crear la VPC subred CIDR con /22 que asignará 1024 direcciones IP, con margen de crecimiento.

VPCopciones de red

Un dominio de SageMaker AI Studio permite configurar la VPC red con una de las siguientes opciones:

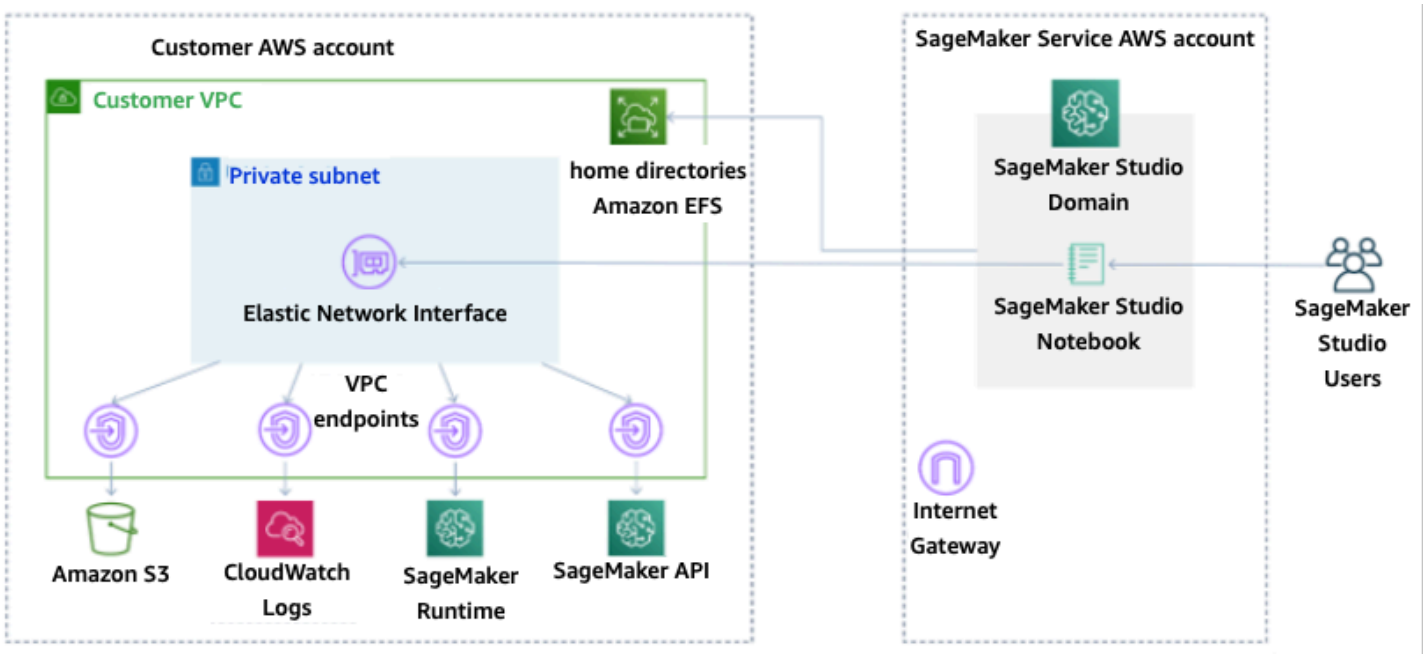
- Solo Internet público
- Sólo VPC

La opción solo para Internet pública permite a API los servicios de SageMaker IA utilizar Internet pública a través de la pasarela de Internet proporcionada en la cuenta de servicio de IAVPC, gestionada por la cuenta de servicio de SageMaker IA, como se muestra en el siguiente diagrama:



Modo predeterminado: acceso a Internet a través de una cuenta de servicio SageMaker AI

La VPCúnica opción desactiva el enrutamiento de Internet desde la cuenta de servicio VPC gestionada por la SageMaker IA y permite al cliente configurar el tráfico que se enrutará a través de los VPC puntos finales, como se muestra en el siguiente diagrama:



VPCúnico modo: sin acceso a Internet a través de la cuenta de servicio SageMaker AI

Para un dominio configurado en modo VPC exclusivo, configure un grupo de seguridad por perfil de usuario para garantizar el aislamiento total de las instancias subyacentes. Cada dominio de una AWS cuenta puede tener su propia VPC configuración y modo de Internet. Para obtener más información sobre la configuración de la VPC red, consulte Connect SageMaker AI Studio Notebooks en VPC a Recursos externos.

Limitaciones

- Una vez creado un dominio de SageMaker AI Studio, no puedes asociar nuevas subredes al dominio.
- El tipo de VPC red (solo o VPC solo Internet pública) no se puede cambiar.

Protección de los datos

Antes de diseñar una carga de trabajo de aprendizaje automático, se deben establecer las prácticas fundamentales que influyen en la seguridad. Por ejemplo, la clasificación de datos proporciona una forma de categorizar los datos en función de los niveles de confidencialidad, y el cifrado protege los datos al hacerlos ininteligibles para el acceso no autorizado. Estos métodos son importantes porque respaldan objetivos como evitar el mal manejo o cumplir con las obligaciones reglamentarias.

SageMaker AI Studio ofrece varias funciones para proteger los datos en reposo y en tránsito. Sin embargo, como se describe en el modelo de responsabilidad AWS compartida, los clientes son responsables de mantener el control sobre el contenido que se aloja en la infraestructura AWS global. En esta sección, describimos cómo los clientes pueden usar esas funciones para proteger sus datos.

Proteja los datos en reposo

Para proteger tus cuadernos de SageMaker AI Studio junto con los datos de creación de modelos y los artefactos de los modelos, la SageMaker IA cifra los cuadernos, así como el resultado de las tareas de entrenamiento y transformación por lotes. SageMaker La IA los cifra de forma predeterminada mediante la clave AWS gestionada de Amazon S3. Esta clave AWS gestionada para Amazon S3 no se puede compartir para el acceso entre cuentas. Para el acceso entre cuentas, especifique su clave administrada por el cliente al crear los recursos de SageMaker IA para poder compartirla para el acceso entre cuentas.

Con SageMaker AI Studio, los datos se pueden almacenar en las siguientes ubicaciones:

- Depósito de S3: cuando se habilita un bloc de notas para compartir, SageMaker AI Studio comparte las instantáneas y los metadatos del bloc de notas en un depósito de S3.
- EFSvolumen: SageMaker AI Studio adjunta un EFS volumen a tu dominio para almacenar libretas y archivos de datos. Este EFS volumen se conserva incluso después de eliminar el dominio.
- EBSvolumen: EBS se adjunta a la instancia en la que se ejecuta el portátil. Este volumen se conserva mientras dure la instancia.

Cifrado en reposo con AWS KMS

- Puede pasar su AWS KMS clave para cifrar un EBS volumen adjunto a cuadernos, equipos de formación, ajustes, trabajos de transformación por lotes y terminales.

- Si no especificas una KMS clave, SageMaker AI cifra tanto los volúmenes del sistema operativo (SO) como los volúmenes de datos de aprendizaje automático con una clave administrada por el sistema. KMS
- Los datos confidenciales que deban cifrarse con una KMS clave por motivos de conformidad deben almacenarse en el volumen de almacenamiento de ML o en Amazon S3, los cuales se pueden cifrar con la KMS clave que especifique.

Protección de los datos en tránsito

SageMaker AI Studio garantiza que los artefactos de los modelos de aprendizaje automático y otros artefactos del sistema estén cifrados tanto en tránsito como en reposo. Las solicitudes a la SageMaker IA API y a la consola se realizan a través de una conexión segura (SSL). Algunos datos dentro de la red en tránsito (dentro de la plataforma de servicios) no están cifrados. Esto incluye:

- Comando y control de las comunicaciones entre el plano de control de servicio y las instancias de trabajo de capacitación (no los datos del cliente).
- Comunicaciones entre nodos en trabajos de entrenamiento y procesamiento distribuido (dentro de la red).

Sin embargo, puedes optar por cifrar la comunicación entre los nodos de un clúster de entrenamiento. La habilitación del cifrado de tráfico entre contenedores puede aumentar el tiempo de capacitación, especialmente si se utilizan algoritmos de aprendizaje profundo distribuidos.

De forma predeterminada, Amazon SageMaker AI realiza trabajos de formación en Amazon VPC para ayudar a mantener tus datos seguros. Puedes añadir otro nivel de seguridad para proteger tus contenedores y datos de entrenamiento configurando una cuenta privadaVPC. Además, puedes configurar tu dominio de SageMaker AI Studio para que se ejecute en modo VPC exclusivo y configurar VPC puntos finales para enrutar el tráfico a través de una red privada sin que el tráfico salga por Internet.

Barandillas de protección de datos

Cifre los volúmenes de alojamiento de SageMaker IA en reposo

Utilice la siguiente política para aplicar el cifrado durante el alojamiento de un punto final de SageMaker IA para realizar inferencias en línea:

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
         "Sid": "Encryption",
         "Effect": "Allow",
         "Action": [
             "sagemaker:CreateEndpointConfig"
         ],
         "Resource": "*",
         "Condition": {
             "Null": {
                 "sagemaker:VolumeKmsKey": "false"
             }
         }
     }
   ]
 }
```

Cifre los cubos S3 utilizados durante la supervisión del modelo

Model Monitoring captura los datos que se envían a su terminal de SageMaker IA y los almacena en un depósito de S3. Al configurar la configuración de captura de datos, debe cifrar el bucket de S3. Actualmente, no existe ningún control compensatorio para ello.

Además de recopilar los resultados de los puntos finales, el servicio de monitorización de modelos comprueba si hay desviaciones respecto a una línea base previamente especificada. Debe cifrar las salidas y los volúmenes de almacenamiento intermedios que se utilizan para controlar la desviación.

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
         "Sid": "Encryption",
         "Effect": "Allow",
         "Action": [
             "sagemaker:CreateMonitoringSchedule",
             "sagemaker:UpdateMonitoringSchedule"
         ],
         "Resource": "*",
         "Condition": {
             "Null": {
```

```
                "sagemaker:VolumeKmsKey": "false",
                "sagemaker:OutputKmsKey": "false"
            }
        }
    }
  ]
}
```

Cifra un volumen de almacenamiento de dominio de SageMaker AI Studio

Aplica el cifrado al volumen de almacenamiento adjunto al dominio de Studio. Esta política requiere que el usuario proporcione un código CMK para cifrar los volúmenes de almacenamiento adjuntos a los dominios de Studio.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EncryptDomainStorage",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateDomain"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "sagemaker:VolumeKmsKey": "false"
                }
            }
        }
    ]
}
```

Cifre los datos almacenados en S3 que se utilizan para compartir blocs de notas

Esta es la política para cifrar todos los datos almacenados en el depósito que se utiliza para compartir libretas entre los usuarios de un SageMaker dominio de AI Studio:

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "EncryptDomainSharingS3Bucket",
            "Effect": "Allow",
            "Action": [
                "sagemaker:CreateDomain",
                "sagemaker:UpdateDomain"
            ],
            "Resource": "*",
            "Condition": {
                "Null": {
                    "sagemaker:DomainSharingOutputKmsKey": "false"
                }
            }
        }
    ]
}
```

Limitaciones

- Una vez creado un dominio, no puedes actualizar el EFS volumen de almacenamiento adjunto con una clave personalizada AWS KMS .
- No puede actualizar los trabajos de formación/procesamiento ni las configuraciones de los terminales con KMS claves una vez que se hayan creado.

Registro y supervisión

Para ayudarle a depurar los trabajos de compilación, los trabajos de procesamiento, los trabajos de formación, los puntos finales, los trabajos de transformación, las instancias de cuadernos y las configuraciones del ciclo de vida de las instancias de cuadernos, todo lo que un contenedor de algoritmos, un contenedor de modelos o una configuración del ciclo de vida de una instancia de cuaderno envíe a stdout o stderr también se envía a Amazon Logs. CloudWatch Puedes monitorizar SageMaker AI Studio con Amazon CloudWatch, que recopila datos sin procesar y los procesa para convertirlos en métricas legibles prácticamente en tiempo real. Estas estadísticas se mantienen durante 15 meses, para que pueda obtener acceso a información histórica y disponer de una mejor perspectiva sobre el desempeño de su aplicación web o servicio.

Iniciar sesión con CloudWatch

Como el proceso de ciencia de datos es intrínsecamente experimental e iterativo, es esencial registrar la actividad como el uso del cuaderno, el tiempo de ejecución de las tareas de entrenamiento/procesamiento, las métricas de entrenamiento y las métricas de servicio de puntos de conexión como, por ejemplo, la latencia de invocación. De forma predeterminada, la SageMaker IA publica las métricas en CloudWatch los registros, y estos registros se pueden cifrar con claves administradas por el cliente mediante. AWS KMS

También puedes usar VPC puntos de conexión a los que enviar registros CloudWatch sin necesidad de utilizar la Internet pública. También puede establecer alarmas que vigilen determinados umbrales y enviar notificaciones o realizar acciones cuando se cumplan dichos umbrales. Para obtener más información, consulta la Guía del CloudWatch usuario de Amazon.

SageMaker AI crea un único grupo de registros para Studio, en`/aws/sagemaker/studio`. Cada perfil de usuario y cada aplicación tiene su propio flujo de registro en este grupo de registro, y los scripts de configuración del ciclo de vida también tienen su propio flujo de registro. Por ejemplo, un perfil de usuario denominado “studio-user” con una aplicación de servidor de Jupyter y con un script de ciclo de vida asociado, y una aplicación de puerta de enlace del kernel de Ciencia de datos tiene los siguientes flujos de registro:

```
/aws/sagemaker/studio/<domain-id>/studio-user/JupyterServer/default
```

```
/aws/sagemaker/studio/<domain-id>/studio-user/JupyterServer/default/
LifecycleConfigOnStart
```

`/aws/sagemaker/studio/<domain-id>/studio-user/KernelGateway/datascience-app`

Para que SageMaker AI pueda enviar los registros CloudWatch en tu nombre, la persona que llame a la Training/Processing/Transform tarea APIs necesitará los siguientes permisos:

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Action": [
                 "logs:CreateLogDelivery",
                 "logs:CreateLogGroup",
                 "logs:CreateLogStream",
                 "logs:DeleteLogDelivery",
                 "logs:Describe*",
                 "logs:GetLogEvents",
                 "logs:GetLogDelivery",
                 "logs:ListLogDeliveries",
                 "logs:PutLogEvents",
                 "logs:PutResourcePolicy",
                 "logs:UpdateLogDelivery"
             ],
             "Resource": "*",
             "Effect": "Allow"
         }
     ]
 }
```

Para cifrar esos registros con una AWS KMS clave personalizada, primero tendrás que modificar la política de claves para que el CloudWatch servicio pueda cifrar y descifrar la clave. Una vez que haya creado una AWS KMS clave de cifrado de registros, modifique la política de claves para incluir lo siguiente:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "logs.region.amazonaws.com"
            },
            "Action": [
```

```
                "kms:Encrypt*",
                "kms:Decrypt*",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:Describe*"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "kms:EncryptionContext:aws:logs:arn": "arn:aws:logs:region:account-
id:*"
                }
            }
        }
    ]
}
```

Ten en cuenta que siempre puedes usar `ArnEquals` y proporcionar un nombre de recurso de Amazon específico (ARN) para el CloudWatch registro que deseas cifrar. Aquí se muestra cómo puede usar esta clave para cifrar todos los registros de una cuenta a efectos de simplicidad. Además, los puntos finales de formación, procesamiento y modelo publican métricas sobre la utilización de la instancia CPU y la memoria, la latencia de invocación del alojamiento, etc. También puedes configurar Amazon SNS para que notifique a los administradores los eventos cuando se superen determinados umbrales. El consumidor de la formación y el procesamiento APIs debe tener los siguientes permisos:

```
{
     "Version": "2012-10-17",
     "Statement": [
         {
             "Action": [
                 "cloudwatch:DeleteAlarms",
                 "cloudwatch:DescribeAlarms",
                 "cloudwatch:GetMetricData",
                 "cloudwatch:GetMetricStatistics",
                 "cloudwatch:ListMetrics",
                 "cloudwatch:PutMetricAlarm",
                 "cloudwatch:PutMetricData",
                 "sns:ListTopics"
             ],
             "Resource": "*",
             "Effect": "Allow",
```

```
            "Condition": {
                "StringLike": {
                    "cloudwatch:namespace": "aws/sagemaker/*"
                }
            }

        },
        {
            "Action": [
                "sns:Subscribe",
                "sns:CreateTopic"
            ],
            "Resource": [
                "arn:aws:sns:*:*:*SageMaker*",
                "arn:aws:sns:*:*:*Sagemaker*",
                "arn:aws:sns:*:*:*sagemaker*"
            ],
            "Effect": "Allow"
        }
    ]
}
```

Audite con AWS CloudTrail

Para mejorar su postura de cumplimiento, audite todo lo que APIs necesite AWS CloudTrail. De forma predeterminada, APIs se registran todas las SageMaker IA AWS CloudTrail. No necesitas ningún IAM permiso adicional para activarla CloudTrail.

Todas las acciones de la SageMaker IA, a excepción de las `InvokeEndpoint` acciones de la IA`InvokeEndpointAsync`, se registran CloudTrail y se documentan en las operaciones. Por ejemplo, las llamadas a las `CreateTrainingJob` `CreateNotebookInstance` acciones y las llamadas generan entradas en los archivos de CloudTrail registro. `CreateEndpoint`

Cada entrada de CloudTrail evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de AWS IAM.
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio. Para ver un ejemplo de evento, consulta el registro de API llamadas de SageMaker IA con CloudTrail la documentación.

De forma predeterminada, CloudTrail registra el nombre de la función de ejecución de Studio del perfil de usuario como identificador de cada evento. Esto funciona si cada usuario tiene su propio rol de ejecución. Si varios usuarios comparten el mismo rol de ejecución, puede usar la `sourceIdentity` configuración para propagar el nombre del perfil de usuario de Studio a CloudTrail. Consulte Supervisión del acceso de los usuarios a los recursos desde Amazon SageMaker AI Studio para activar la `sourceIdentity` función. En un espacio compartido, todas las acciones hacen referencia al espacio ARN como fuente y no es posible realizar una auditoría exhaustiva`sourceIdentity`.

Atribución de costes

SageMaker AI Studio ha incorporado funciones para ayudar a los administradores a realizar un seguimiento del gasto de sus dominios individuales, espacios compartidos y usuarios.

Etiquetado automatizado

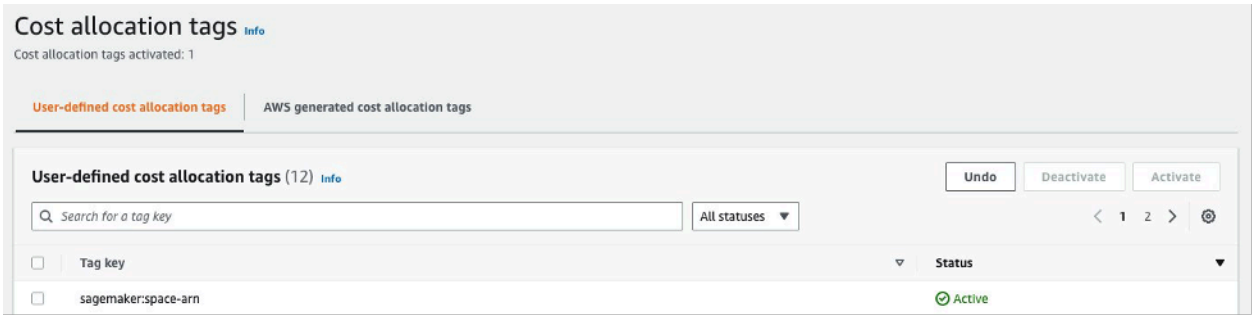
SageMaker AI Studio ahora etiqueta automáticamente SageMaker los nuevos recursos, como los trabajos de formación, los trabajos de procesamiento y las aplicaciones del núcleo, con sus respectivos atributos`sagemaker:domain-arn`. A un nivel más detallado, la SageMaker IA también etiqueta el recurso con `sagemaker:user-profile-arn` o `sagemaker:space-arn` para designar al creador principal del recurso.

SageMaker Los EFS volúmenes de dominio de IA se etiquetan `ManagedByAmazonSageMakerResource` con una clave denominada con el valor del dominioARN. No tienen etiquetas granulares para comprender el uso del espacio por usuario. Sin embargo, los administradores pueden adjuntar el EFS volumen a una EC2 instancia para realizar una supervisión personalizada.

Supervisión de costos

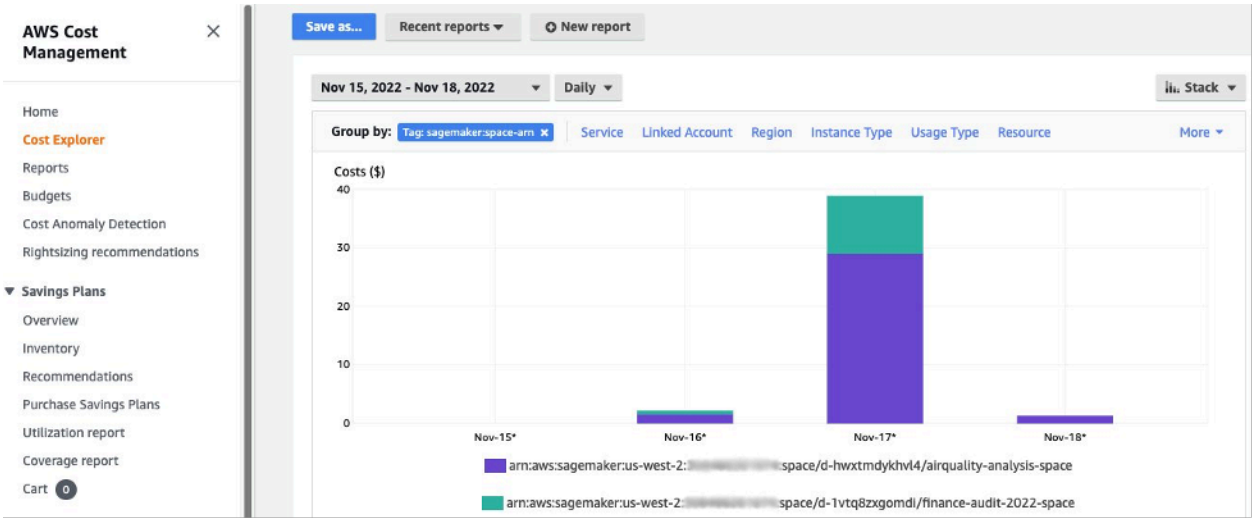
Las etiquetas automatizadas permiten a los administradores realizar un seguimiento, elaborar informes y supervisar su gasto en aprendizaje automático mediante out-of-the-box soluciones como AWS Cost ExplorerAWS Budgets, por ejemplo, soluciones personalizadas basadas en los datos de los informes de AWS costes y uso ()CURs.

Para utilizar las etiquetas adjuntas para el análisis de costes, primero hay que activarlas en la sección de etiquetas de asignación de costes de la AWS Billing consola. Las etiquetas pueden tardar hasta 24 horas en aparecer en el panel de etiquetas de asignación de costes, por lo que tendrás que crear un recurso de SageMaker IA antes de habilitarlas.



Espacio ARN activado como etiquetas de asignación de costes en Cost Explorer

Una vez que haya activado una etiqueta de asignación de costos, AWS empezará a rastrear los recursos etiquetados y, después de 24 a 48 horas, las etiquetas aparecerán como filtros seleccionables en el explorador de costos.



Los costos se agrupan por espacio compartido para un dominio de muestra

Control de costos

Cuando se incorpora el primer usuario de SageMaker AI Studio, SageMaker AI crea un EFS volumen para el dominio. Este EFS volumen conlleva costes de almacenamiento, ya que las libretas y los archivos de datos se almacenan en el directorio principal del usuario. Cuando el usuario lanza los blocs de notas Studio, se lanzan para las instancias de procesamiento que ejecutan los blocs de notas. Consulta los precios de Amazon SageMaker AI para obtener un desglose detallado de los costes.

Los administradores pueden controlar los costos de cómputo especificando la lista de instancias que un usuario puede crear, utilizando IAM las políticas que se mencionan en la sección sobre barreras comunes. Además, recomendamos a los clientes que utilicen la extensión de apagado automático SageMaker AI Studio para ahorrar costos al cerrar automáticamente las aplicaciones inactivas. Esta extensión de servidor consulta periódicamente las aplicaciones en ejecución por perfil de usuario y cierra las aplicaciones inactivas en función del tiempo de espera establecido por el administrador.

Para configurar esta extensión para todos los usuarios de tu dominio, puedes usar una configuración de ciclo de vida tal como se describe en la sección de personalización. Además, también puedes

usar el comprobador de extensiones para asegurarte de que todos los usuarios de tu dominio tengan la extensión instalada.

Personalización

Configuración del ciclo de vida

Las configuraciones del ciclo de vida son scripts de shell iniciados por eventos del ciclo de vida de SageMaker AI Studio, como el inicio de un nuevo bloc de notas de SageMaker AI Studio. Puedes usar estos scripts de shell para automatizar la personalización de tus entornos de SageMaker AI Studio, como la instalación de paquetes personalizados, la extensión Jupyter para el cierre automático de aplicaciones de notebook inactivas y la configuración de Git. Para obtener instrucciones detalladas sobre cómo crear configuraciones de ciclo de vida, consulte este blog: Personalice Amazon SageMaker AI Studio mediante configuraciones de ciclo de vida.

Imágenes personalizadas para las libretas SageMaker AI Studio

Los cuadernos Studio vienen con un conjunto de imágenes prediseñadas, que consisten en Amazon AI SageMaker Python SDK y la última versión del motor de IPython ejecución o kernel. Con esta función, puedes llevar tus propias imágenes personalizadas a las libretas Amazon SageMaker AI. Estas imágenes estarán entonces disponibles para todos los usuarios autenticados en el dominio.

Los desarrolladores y los científicos de datos pueden necesitar imágenes personalizadas para varios casos de uso diferentes:

- Acceda a versiones específicas o más recientes de marcos de aprendizaje automático populares TensorFlow, comoMXNet, PyTorch, u otros.
- Incorpora códigos o algoritmos personalizados desarrollados localmente a las libretas de SageMaker AI Studio para agilizar la iteración y el entrenamiento de modelos.
- Acceda a lagos de datos o almacenes de datos locales mediante. APIs Los administradores deben incluir los controladores correspondientes en la imagen.
- Acceso a un tiempo de ejecución de backend (también denominado núcleo), distinto de IPython (como R, Julia u otros). También puede utilizar el enfoque descrito para instalar un núcleo personalizado.

Para obtener instrucciones detalladas sobre cómo crear una imagen personalizada, consulte Crear una imagen de SageMaker IA personalizada.

JupyterLab extensiones

Con SageMaker AI Studio JuypterLab 3 Notebook, puedes aprovechar la creciente comunidad de extensiones de código abierto JupyterLab. En esta sección se destacan algunas que se adaptan perfectamente al flujo de trabajo de los desarrolladores de SageMaker IA, pero te animamos a que busques entre las extensiones disponibles o incluso que crees las tuyas propias.

JupyterLab La versión 3 ahora facilita considerablemente el proceso de empaquetar e instalar extensiones. Puede instalar las extensiones antes mencionadas mediante scripts bash. Por ejemplo, en SageMaker AI Studio, abre el terminal del sistema desde el lanzador de Studio y ejecuta los siguientes comandos. Además, puedes automatizar la instalación de estas extensiones mediante configuraciones de ciclo de vida para que persistan entre los reinicios de Studio. Puedes configurarlo para todos los usuarios del dominio o a nivel de usuario individual.

Por ejemplo, para instalar una extensión para un navegador de archivos Amazon S3, ejecute los siguientes comandos en el terminal del sistema y asegúrese de actualizar el navegador:

```
conda init
conda activate studio
pip install jupyterlab_s3_browser
jupyter serverextension enable --py jupyterlab_s3_browser
conda deactivate
restart-jupyter-server
```

Para obtener más información sobre la administración de extensiones, incluido cómo escribir configuraciones del ciclo de vida que funcionen para las versiones 1 y 3 de los JupyterLab portátiles para garantizar la compatibilidad con versiones anteriores, consulte Instalación JupyterLab y extensiones de Jupyter Server.

Repositorios de Git

SageMaker AI Studio viene preinstalada con una extensión Git de Jupyter para que los usuarios puedan acceder a un URL repositorio Git personalizado, clonarlo EFS en su directorio, enviar cambios y ver el historial de confirmaciones. Los administradores pueden configurar los repositorios de git sugeridos a nivel de dominio para que los usuarios finales puedan verlos en forma de listas desplegables. Consulta Adjuntar repositorios de Git sugeridos a Studio para obtener up-to-date instrucciones.

Si un repositorio es privado, la extensión le pedirá al usuario que introduzca sus credenciales en el terminal mediante la instalación estándar de git. Como alternativa, el usuario puede almacenar las credenciales ssh en su EFS directorio individual para facilitar la administración.

Entorno Conda

SageMaker Las libretas de AI Studio utilizan Amazon EFS como capa de almacenamiento persistente. Los científicos de datos pueden utilizar el almacenamiento persistente para crear entornos conda personalizados y utilizar estos entornos para crear núcleos. Estos núcleos están respaldados por EFS y son persistentes entre el reinicio del kernel, la aplicación o el estudio. Studio selecciona automáticamente todos los entornos válidos como KernelGateway núcleos.

El proceso de creación de un entorno conda es sencillo para un científico de datos, pero los núcleos tardan aproximadamente un minuto en rellenarse en el selector de núcleos. Para crear un entorno, ejecute lo siguiente en una terminal del sistema:

```
mkdir -p ~/.conda/envs
conda create --yes -p ~/.conda/envs/custom
conda activate ~/.conda/envs/custom
conda install -y ipykernel
conda config --add envs_dirs ~/.conda/envs
```

Para obtener instrucciones detalladas, consulte la sección Persist Conda entre los entornos y el EFS volumen de Studio en Cuatro enfoques para administrar paquetes de Python en los cuadernos de Amazon SageMaker Studio.

Conclusión

En este documento técnico, analizamos varias prácticas recomendadas en áreas como el modelo operativo, la administración de dominios, la administración de identidades, la administración de permisos, la administración de redes, el registro, la supervisión y la personalización para permitir a los administradores de la plataforma configurar y administrar la plataforma SageMaker AI Studio.

Apéndice

Comparación de varios arrendatarios

Tabla 2: Comparación de varios arrendatarios

Multidominio	Cuenta múltiple	Control de acceso basado en atributos (ABAC) dentro de un único dominio
El aislamiento de los recursos se consigue mediante etiquetas. SageMaker AI Studio etiqueta automátic amente todos los recursos con el dominio ARN y el perfil/es pacio de usuario. ARN	Cada inquilino está en su propia cuenta, por lo que hay un aislamiento absoluto de los recursos.	El aislamiento de los recursos se logra mediante etiquetas. Los usuarios deben gestionar el etiquetado de los recursos creados paraABAC.
La lista APIs no puede estar restringida por etiquetas. El filtrado de los recursos a través de la interfaz de usuario se realiza en los espacios compartidos; sin embargo, API las llamadas de List realizadas a través del Boto3 AWS CLI o del Boto3 SDK mostrarán los recursos de la región.	También es posible APIs aislar las listas, ya que los inquilinos están en sus cuentas dedicadas.	La lista APIs no puede estar restringida por etiquetas. Enumere API las llamadas realizadas a través del Boto3 AWS CLI o el Boto3 SDK mostrará una lista de los recursos de la región.
SageMaker Los costes de cómputo y almacenamiento de AI Studio por inquilino se pueden monitorizar fácilmente utilizando Domain ARN como etiqueta de asignación de costes.	SageMaker Los costes de cómputo y almacenamiento de AI Studio por inquilino son fáciles de supervisar con una cuenta dedicada.	SageMaker Los costes de cómputo de AI Studio por inquilino deben calcularse mediante etiquetas personali zadas.

Multidominio	Cuenta múltiple	Control de acceso basado en atributos (ABAC) dentro de un único dominio
		SageMaker Los costos de almacenamiento de AI Studio no se pueden monitorear por dominio, ya que todos los inquilinos comparten el mismo EFS volumen.
Las cuotas de servicio se establecen a nivel de cuenta, por lo que un solo inquilino podría seguir consumiendo todos los recursos.	Las cuotas de servicio se pueden establecer a nivel de cuenta para cada inquilino.	Las cuotas de servicio se establecen a nivel de cuenta, por lo que un solo inquilino podría seguir consumiendo todos los recursos.
El escalamiento a varios inquilinos se puede lograr mediante la infraestructura como código (IaC) o Service Catalog.	La ampliación a varios inquilinos implica Organizat ions y la venta de varias cuentas.	Scaling necesita un rol de inquilino específico para cada nuevo inquilino, y los perfiles de usuario deben etiquetarse manualmente con los nombres de los inquilinos.
La colaboración entre los usuarios de un inquilino es posible a través de los espacios compartidos.	La colaboración entre un usuario y un inquilino es posible a través de espacios compartidos.	Todos los inquilinos tendrán acceso al mismo espacio compartido para la colaborac ión.

SageMaker Copia de seguridad y recuperación de dominios de AI Studio

En caso de una EFS eliminación accidental o si es necesario volver a crear un dominio debido a cambios en la red o la autenticación, sigue estas instrucciones.

Opción 1: Realice una copia de seguridad desde una versión existente utilizando EFS EC2

SageMaker Respaldo del dominio de Studio

1. Muestra los perfiles de usuario y los espacios de SageMaker Studio (CLI, SDK).
2. Asigne perfiles o espacios de usuario a UIDs uno. EFS
   a. Para cada usuario de la lista de users/spaces, describe the user profile/space (CLI, SDK).
   b. Asigne el perfil/espacio de usuario a. `HomeEfsFileSystemUid`
   c. Asigne el perfil de usuario a `UserSettings['ExecutionRole']` si los usuarios tienen funciones de ejecución distintas.
   d. Identifique el rol de ejecución predeterminado de Space.
3. Cree un nuevo dominio y especifique la función de ejecución de Space predeterminada.
4. Cree perfiles de usuario y espacios.
   - Para cada usuario de la lista de usuarios, cree un perfil de usuario (CLI, SDK) mediante la asignación de funciones de ejecución.
5. Cree un mapeo para el nuevo EFS yUIDs.
   a. Para cada usuario de la lista de usuarios, describa el perfil de usuario (CLI, SDK).
   b. Asigne el perfil de usuario a`HomeEfsFileSystemUid`.
6. Si lo desea, elimine todas las aplicaciones, los perfiles de usuario y los espacios y, a continuación, elimine el dominio.

Copia de seguridad de EFS

Para realizar una copia de seguridadEFS, siga las instrucciones siguientes:

1. Lanza la EC2 instancia y adjunta los grupos de seguridad entrantes y salientes del antiguo dominio de SageMaker Studio a la nueva EC2 instancia (permite que el NFS tráfico pase por TCP el puerto 2049). Consulte Connect SageMaker Studio Notebooks en una VPC sección Recursos externos.
2. Monte el EFS volumen de SageMaker Studio en la nueva EC2 instancia. Consulte Montaje de sistemas de EFS archivos.
3. Copie los archivos al almacenamiento EBS local: `>sudo cp -rp /efs /studio-backup:`
   a. Adjunta los nuevos grupos de seguridad de dominio a la EC2 instancia.

b. Monta el nuevo EFS volumen en la EC2 instancia.

c. Copie los archivos al nuevo EFS volumen.

d. Para cada usuario de la colección de usuarios:

i. Cree el directorio: `mkdir new_uid`.

ii. Copie los archivos del UID directorio anterior al nuevoUID.

iii. Cambiar la propiedad de todos los archivos: `chown <new_UID>` de todos los archivos.

Opción 2: Realice una copia de seguridad de los existentes EFS mediante S3 y la configuración del ciclo de vida

1. Consulte Migrar su trabajo a una instancia de Amazon SageMaker Notebook con Amazon Linux 2.
2. Cree un bucket de S3 para la copia de seguridad (por ejemplo `>studio-backup`.
3. Enumere todos los perfiles de usuario con funciones de ejecución.
4. En el dominio de SageMaker Studio actual, establece un LCC script predeterminado a nivel de dominio.
   - En elLCC, copia todo en `/home/sagemaker-user` el prefijo del perfil de usuario en S3 (por ejemplo,`s3://studio-backup/studio-user1`).
5. Reinicie todas las aplicaciones predeterminadas de Jupyter Server (para LCC que se ejecuten).
6. Elimine todas las aplicaciones, perfiles de usuario y dominios.
7. Crea un nuevo dominio de SageMaker Studio.
8. Crea nuevos perfiles de usuario a partir de la lista de perfiles de usuario y funciones de ejecución.
9. Configure un LCC a nivel de dominio:
   - En elLCC, copie todo el prefijo del perfil de usuario en S3 para `/home/sagemaker-user`
10. Cree aplicaciones predeterminadas de Jupyter Server para todos los usuarios con la LCCconfiguración (CLI,). SDK

SageMaker Acceso a Studio mediante aserción SAML

Configuración de la solución:

1. Cree una SAML aplicación en su IdP externo.
2. Configure el IdP externo como proveedor de identidad en. IAM

3. Cree una función `SAMLValidator` Lambda a la que pueda acceder el IdP (a través de una función URL o puerta de enlace). API
4. Cree una función `GeneratePresignedUrl` Lambda y una API puerta de enlace para acceder a la función.
5. Cree una IAM función que los usuarios puedan asumir al invocar la puerta de enlace. API Esta función debe pasarse en forma de SAML aserción como atributo en el siguiente formato:
   - Nombre del atributo: https://aws.amazon.com/SAML/ Atributos/Rol
   - Valor de atributo: `<IdentityProviderARN>`, `<RoleARN>`
6. Actualice el punto final de SAML Assertion Consumer Service (ACS) a la invocación. `SAMLValidator` URL

SAMLCódigo de ejemplo del validador:

```
import requests
import os
import boto3
from urllib.parse import urlparse, parse_qs
import base64
import requests
from aws_requests_auth.aws_auth import AWSRequestsAuth
import json


# Config for calling AssumeRoleWithSAML
idp_arn = "arn:aws:iam::0123456789:saml-provider/MyIdentityProvider"
api_gw_role_arn = 'arn:aws:iam:: 0123456789:role/APIGWAccessRole'
studio_api_url = "abcdef.execute-api.us-east-1.amazonaws.com"
studio_api_gw_path = "https://" + studio_api_url + "/Prod "

# Every customer will need to get SAML Response from the POST call
def get_saml_response(event):
    saml_response_uri = base64.b64decode(event['body']).decode('ascii')
    request_body = parse_qs(saml_response_uri)
    print(f"b64 saml response: {request_body['SAMLResponse'][0]}")
    return request_body['SAMLResponse'][0]


def lambda_handler(event, context):
    sts = boto3.client('sts')
```

```
    # get temporary credentials
    response = sts.assume_role_with_saml(
                    RoleArn=api_gw_role_arn,
                    PrincipalArn=durga_idp_arn,
                    SAMLAssertion=get_saml_response(event)
                )
    auth = AWSRequestsAuth(aws_access_key=response['Credentials']['AccessKeyId'],
                      aws_secret_access_key=response['Credentials']['SecretAccessKey'],
                      aws_host=studio_api_url,
                      aws_region='us-west-2',
                      aws_service='execute-api',
                      aws_token=response['Credentials']['SessionToken'])

    presigned_response = requests.post(
        studio_api_gw_path,
        data=saml_response_data,
        auth=auth)

    return presigned_response
```

Documentación adicional

- Configuración de entornos de aprendizaje automático seguros y bien gobernados en AWS (AWS blog)
- Configuración de Amazon SageMaker AI Studio para equipos y grupos con aislamiento total de recursos (AWS blog)
- Cómo incorporar Amazon SageMaker AI Studio a AWS SSO Okta Universal Directory (blog)AWS
- Cómo configurar la SAML versión 2.0 para la federación de AWS cuentas (documentación de Okta)
- Creación de una plataforma de machine learning empresarial segura en AWS (guía técnica de AWS)
- Personalice Amazon SageMaker AI Studio mediante configuraciones de ciclo de vida (AWS blog)
- Cómo incorporar tu propia imagen de contenedor personalizada a las libretas de Amazon SageMaker AI Studio (AWS blog)
- Cree plantillas de proyectos de SageMaker IA personalizadas: prácticas recomendadas (AWS blog)
- Implementación de un modelo multicuenta con Amazon SageMaker AI Pipelines (blog)AWS
- Parte 1: Cómo NatWest Group creó una MLOps plataforma escalable, segura y sostenible (blog)AWS
- Proteja Amazon SageMaker AI Studio prefirmado, URLs parte 1: Infraestructura fundamental (blog)AWS

Colaboradores

Los colaboradores de este documento son:

- Ram Vittal, arquitecto de soluciones ML, Amazon Web Services
- Sean Morgan, arquitecto de soluciones de aprendizaje automático, Amazon Web Services
- Durga Sury, arquitecta de soluciones de aprendizaje automático, Amazon Web Services

Un agradecimiento especial a las siguientes personas que aportaron ideas, revisiones y perspectivas:

- Alessandro Cerè, arquitecto de soluciones de inteligencia artificial y aprendizaje automático, Amazon Web Services
- Sumit Thakur, líder de productos de SageMaker IA, Amazon Web Services
- Han Zhang, ingeniero sénior de desarrollo de software, Amazon Web Services
- Bhadrinath Pani, ingeniero de desarrollo de software, Amazon Web Services, Amazon Web Services

Revisiones del documento

Para recibir notificaciones sobre las actualizaciones de este documento técnico, suscríbase a la fuente RSS.

Cambio	Descripción	Fecha
Documento técnico actualizado	Se han corregido los enlaces rotos y numerosos cambios editoriales.	25 de abril de 2023
Publicación inicial	Documento técnico publicado.	19 de octubre de 2022

Avisos

Es responsabilidad de los clientes realizar su propia evaluación independiente de la información que contiene este documento. El presente documento: (a) tiene solo fines informativos, (b) representa las ofertas y prácticas actuales de los productos de AWS, que están sujetas a cambios sin previo aviso, y (c) no supone ningún compromiso ni garantía por parte de AWS y sus filiales, proveedores o licenciantes. Los productos o servicios de AWS se proporcionan “tal cual”, sin garantías, afirmaciones ni condiciones de ningún tipo, ya sean expresas o implícitas. Las responsabilidades y obligaciones de AWS con respecto a sus clientes se controlan mediante los acuerdos de AWS y este documento no forma parte ni modifica ningún acuerdo entre AWS y sus clientes.

Glosario de AWS

Para ver la terminología más reciente de AWS, consulte el Glosario de AWS en la Referencia de Glosario de AWS.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.